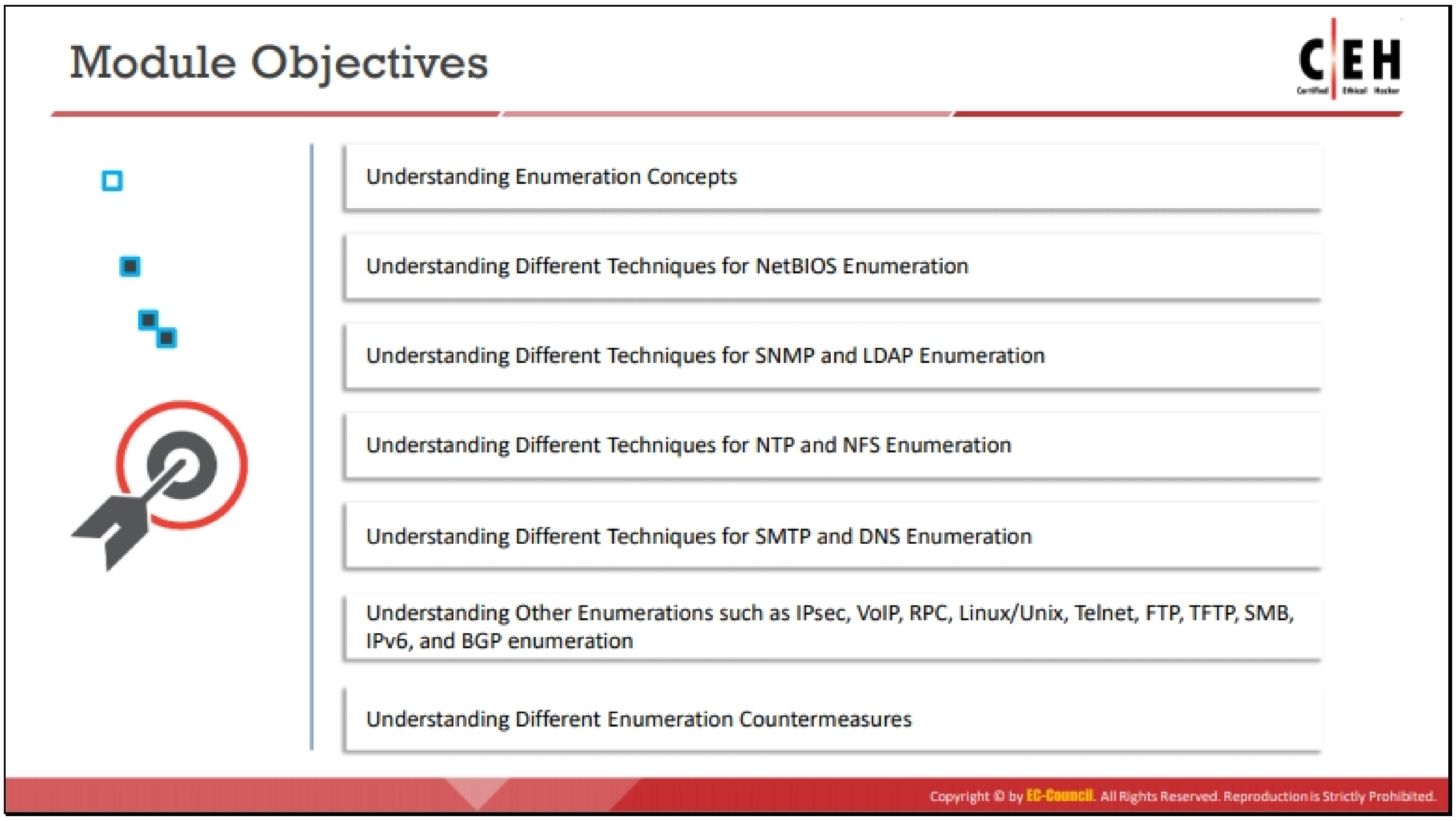
C|EH™
Certified Ethical Hacker

Module 04:
Enumeration



Module Objectives

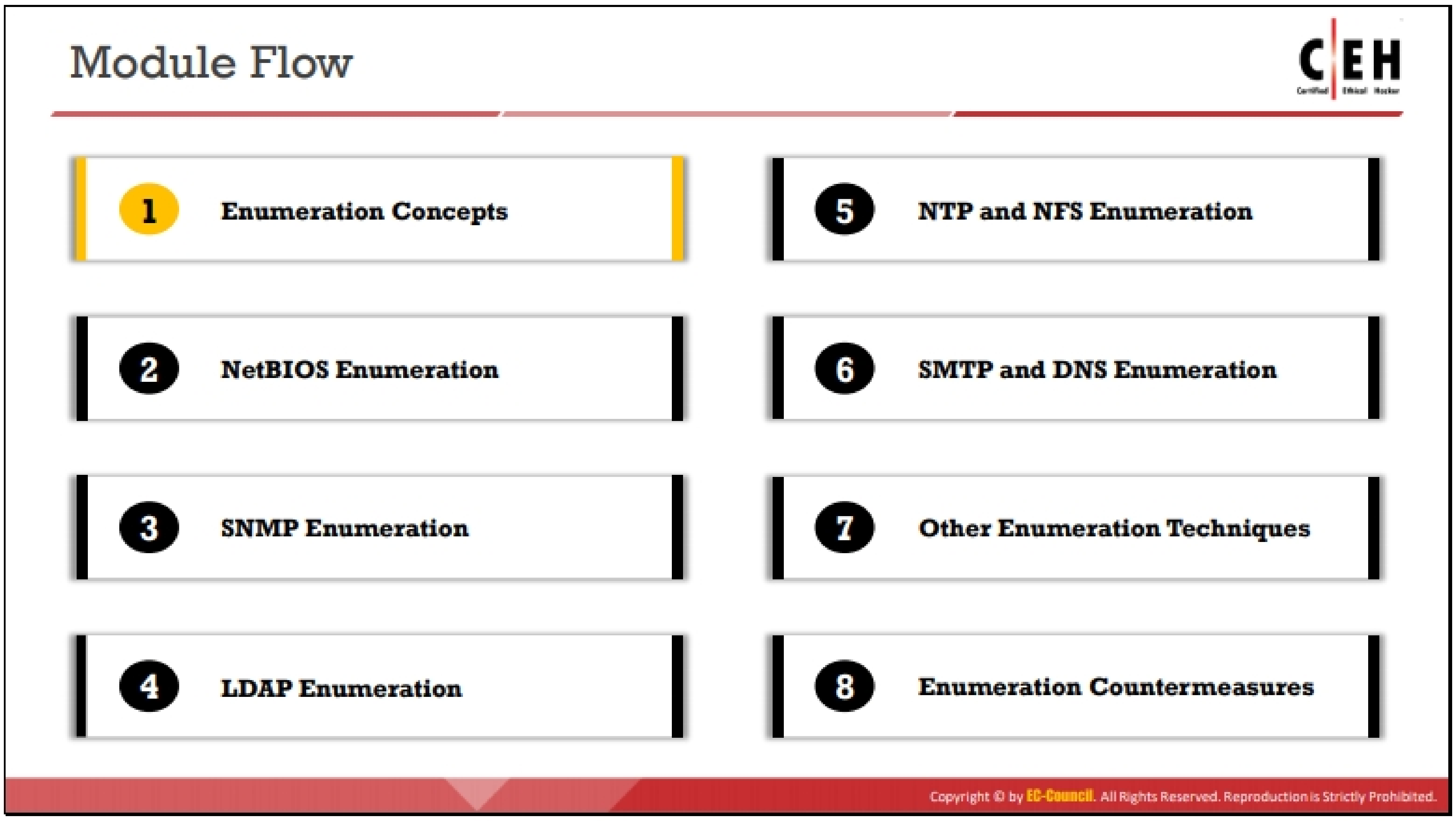
- Understanding Enumeration Concepts
- Understanding Different Techniques for NetBIOS Enumeration
- Understanding Different Techniques for SNMP and LDAP Enumeration
- Understanding Different Techniques for NTP and NFS Enumeration
- Understanding Different Techniques for SMTP and DNS Enumeration
- Understanding Other Enumerations such as IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration
- Understanding Different Enumeration Countermeasures

Module Objectives

In the previous modules, you learned about footprinting and network scanning. This module covers the next phase, enumeration. We start with an introduction to enumeration concepts. Subsequently, the module provides insight into different techniques for Network Basic Input/Output System (NetBIOS), Simple Network Management Protocol (SNMP), Lightweight Directory Access Protocol (LDAP), Network Time Protocol (NTP), Network File System (NFS), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), Internet Protocol Security (IPsec), Voice over Internet Protocol (VoIP), remote procedure call (RPC), Linux/Unix, Telnet, File Transfer Protocol (FTP), Trivial FTP (TFTP), Server Message Block (SMB), Internet Protocol version 6 (IPv6), and Border Gateway Protocol (BGP) enumeration. The module ends with an overview of enumeration countermeasures.

At the end of this module, you will be able to:

- Describe enumeration concepts
- Explain different techniques for NetBIOS enumeration
- Explain different techniques for SNMP enumeration
- Explain different techniques for LDAP enumeration
- Explain different techniques for NTP enumeration
- Explain different techniques for NFS enumeration
- Explain different techniques for SMTP and DNS enumeration
- Explain other enumeration techniques such as IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration
- Apply enumeration countermeasures



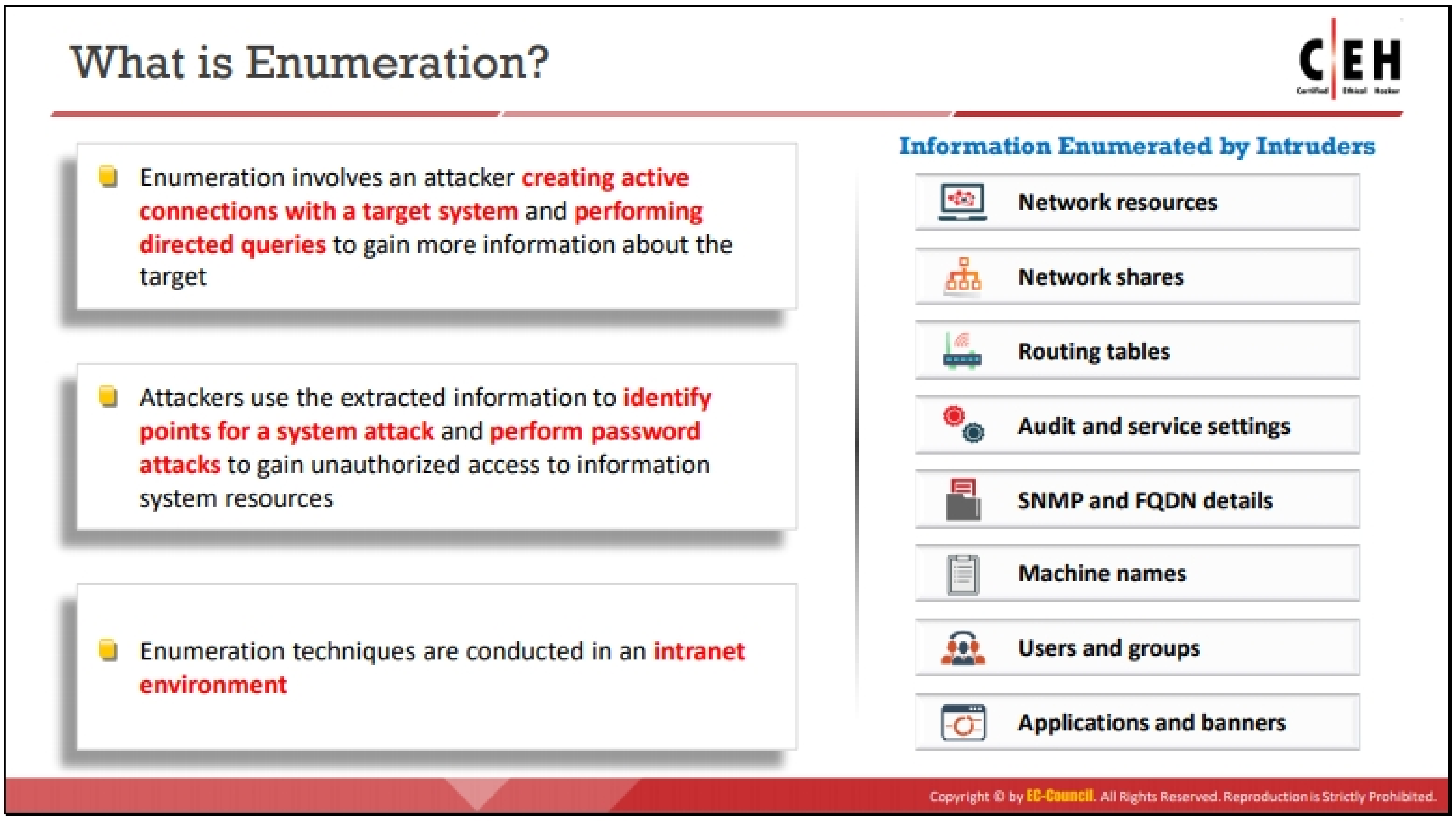
Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

Enumeration Concepts

In the enumeration phase, attackers enumerate usernames and other information on the groups, network shares, and services of networked computers. This information helps attackers identify vulnerabilities in the target network and exploit them to hack the system.

Different sections of this module deal with the enumeration of different services and ports. Before discussing the actual enumeration process, we introduce concepts related to enumeration.



What is Enumeration?

- Enumeration involves an attacker **creating active connections with a target system** and **performing directed queries** to gain more information about the target
- Attackers use the extracted information to **identify points for a system attack** and **perform password attacks** to gain unauthorized access to information system resources
- Enumeration techniques are conducted in an **intranet environment**

Information Enumerated by Intruders

- **Network resources**
- **Network shares**
- **Routing tables**
- **Audit and service settings**
- **SNMP and FQDN details**
- **Machine names**
- **Users and groups**
- **Applications and banners**

What is Enumeration?

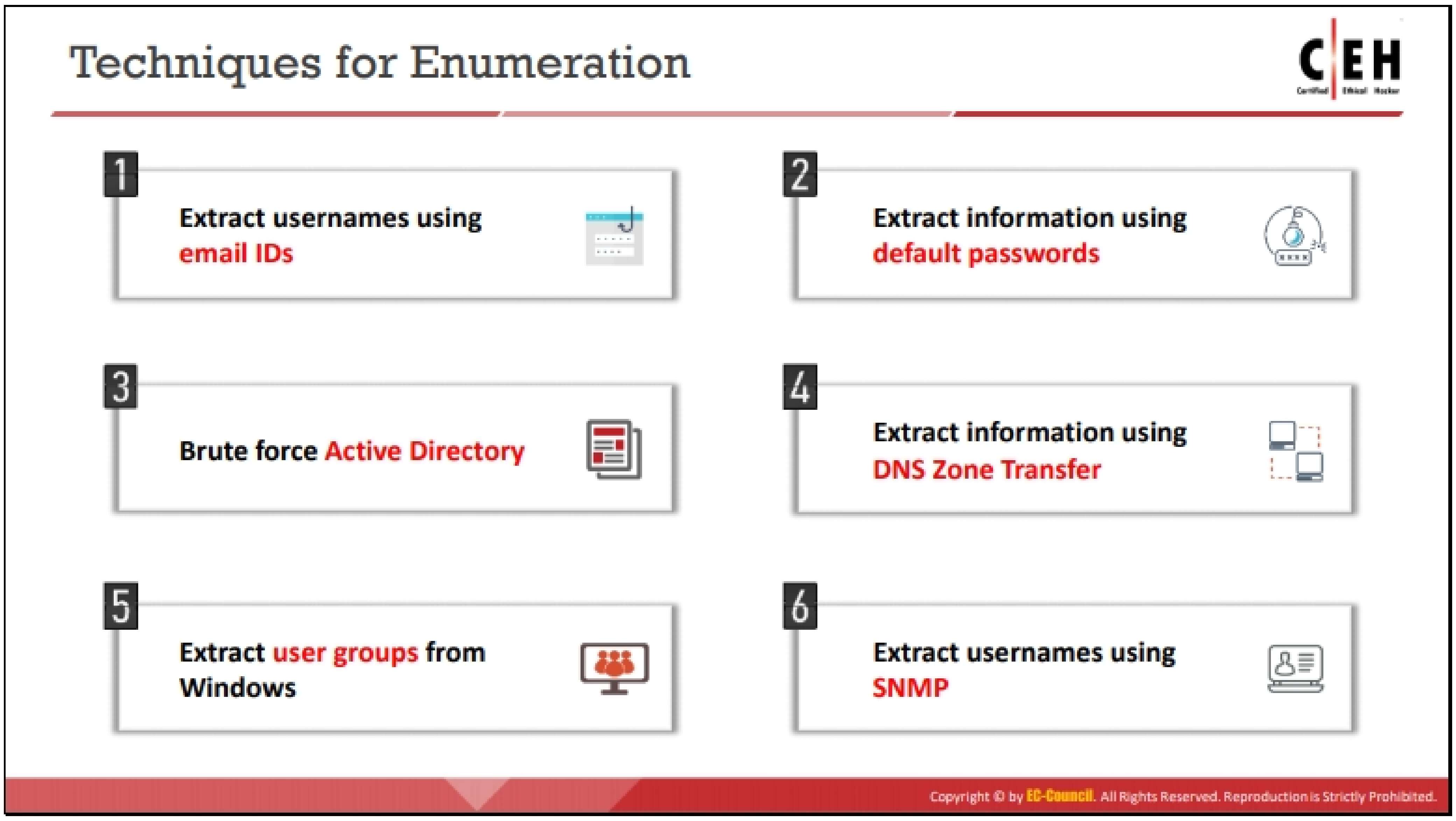
Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network. In the enumeration phase, an attacker creates active connections with the system and sends directed queries to gain more information about the target. The attacker uses the information collected using enumeration to identify vulnerabilities in the system security, which help them exploit the target system. In turn, enumeration allows the attacker to perform password attacks to gain unauthorized access to information system resources. Enumeration techniques work in an intranet environment.

In particular, enumeration allows the attacker to collect the following information:

- Network resources
- Network shares
- Routing tables
- Audit and service settings
- SNMP and fully qualified domain name (FQDN) details
- Machine names
- Users and groups
- Applications and banners

During enumeration, attackers may stumble upon a remote inter-process communication (IPC) share, such as IPC$ in Windows, which they can probe further to connect to an administrative share by brute-forcing admin credentials and obtain complete information about the file-system listing that the share represents.

The previous modules highlighted how attackers gather necessary information about a target without any illegal activity. However, enumeration activities may be illegal depending on the organization's policies and the laws that are in effect. An ethical hacker or pen tester should always acquire proper authorization before performing enumeration.



Techniques for Enumeration

1. Extract usernames using **email IDs**
2. Extract information using **default passwords**
3. Brute force **Active Directory**
4. Extract information using **DNS Zone Transfer**
5. Extract **user groups** from Windows
6. Extract usernames using **SNMP**

Techniques for Enumeration

The following techniques are used to extract information about a target.

- **Extract usernames using email IDs**

  Every email address contains two parts, a username and a domain name, in the format "username@domainname."

- **Extract information using default passwords**

  Many online resources provide a list of default passwords assigned by manufacturers to their products. Users often ignore recommendations to change the default usernames and passwords provided by the manufacturer or developer of a product. This eases an attacker's task of enumerating and exploiting the target system.

- **Brute force Active Directory**

  Microsoft Active Directory is susceptible to username enumeration at the time of user-supplied input verification. This is a design error in the Microsoft Active Directory implementation. If a user enables the "logon hours" feature, then all the attempts at service authentication result in different error messages. Attackers take advantage of this to enumerate valid usernames. An attacker who succeeds in extracting valid usernames can conduct a brute-force attack to crack the respective passwords.

- **Extract information using DNS Zone Transfer**

  A network administrator can use DNS zone transfer to replicate DNS data across several DNS servers or back up DNS files. For this purpose, the administrator needs to execute a specific zone-transfer request to the name server. If the name server permits zone transfer, it will convert all the DNS names and IP addresses hosted by that server to ASCII text.

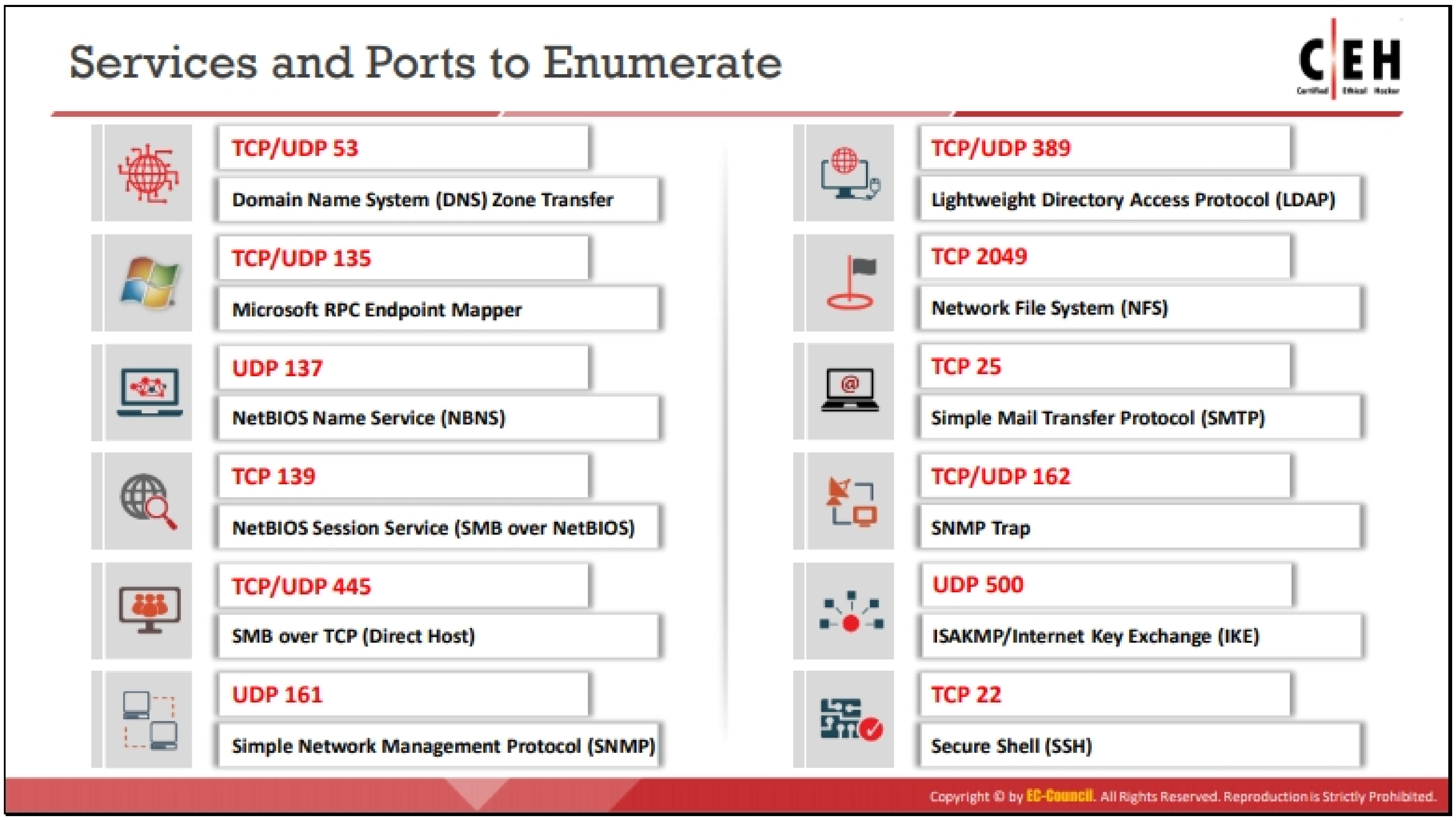
If the network administrators did not configure the DNS server properly, the DNS zone transfer can be an effective method to obtain information about the organization's network. This information may include lists of all named hosts, sub-zones, and related IP addresses. A user can perform DNS zone transfer using nslookup and dig commands.

- **Extract user groups from Windows**

  To extract user groups from Windows, the attacker should have a registered ID as a user in the Active Directory. The attacker can then extract information from groups in which the user is a member by using the Windows interface or command-line method.

- **Extract usernames using SNMP**

  Attackers can easily guess read-only or read-write community strings by using the SNMP application programming interface (API) to extract usernames.



Services and Ports to Enumerate

TCP/UDP 53	Domain Name System (DNS) Zone Transfer
TCP/UDP 135	Microsoft RPC Endpoint Mapper
UDP 137	NetBIOS Name Service (NBNS)
TCP 139	NetBIOS Session Service (SMB over NetBIOS)
TCP/UDP 445	SMB over TCP (Direct Host)
UDP 161	Simple Network Management Protocol (SNMP)
TCP/UDP 389	Lightweight Directory Access Protocol (LDAP)
TCP 2049	Network File System (NFS)
TCP 25	Simple Mail Transfer Protocol (SMTP)
TCP/UDP 162	SNMP Trap
UDP 500	ISAKMP/Internet Key Exchange (IKE)
TCP 22	Secure Shell (SSH)

Services and Ports to Enumerate

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) manage data communications between terminals in a network.

TCP is a connection-oriented protocol capable of carrying messages or emails over the Internet. It provides a reliable multi-process communication service in a multi-network environment. The features and functions of TCP include the following:

- Supports acknowledgement for receiving data through a sliding window acknowledgement system
- Offers automatic retransmission of lost or acknowledged data
- Allows addressing and multiplexing of data
- A connection can be established, managed, or terminated
- Offers quality-of-service transmission
- Offers congestion management and flow control

UDP is a connectionless protocol that carries short messages over a computer network. It provides unreliable service. The applications of UDP include the following:

- Audio streaming
- Videoconferencing and teleconferencing

Services and TCP/UDP ports that can be enumerated include the following.

- **TCP/UDP 53: DNS Zone Transfer**

  The DNS resolution process establishes communication between DNS clients and DNS servers. DNS clients send DNS messages to DNS servers listening on UDP port 53. If the DNS message size exceeds the default size of UDP (512 octets), the response contains only the data that UDP can accommodate, and the DNS server sets a flag to indicate the truncated response. The DNS client can now resend the request via TCP over port 53 to the DNS server. In this approach, the DNS server uses UDP as a default protocol. In the case of lengthy queries for which UDP fails, TCP is used as a failover solution. Malware such as ADM worm and Bonk Trojan uses port 53 to exploit vulnerabilities within DNS servers, helping intruders launch attacks.

- **TCP/UDP 135: Microsoft RPC Endpoint Mapper**

  Source: *https://technet.microsoft.com*

  RPC is a protocol used by a client system to request a service from a server. An endpoint is the protocol port on which the server listens for the client's RPCs. The RPC Endpoint Mapper enables RPC clients to determine the port number currently assigned to a specific RPC service. There is a flaw in the part of RPC that exchanges messages over TCP/IP. The incorrect handling of malformed messages causes failure. This affects the RPC Endpoint Mapper, which listens on TCP/IP port 135. This vulnerability could allow an attacker to send RPC messages to the RPC Endpoint Mapper process on a server to launch a denial-of-service (DoS) attack.

- **UDP 137: NetBIOS Name Service (NBNS)**

  NBNS, also known as the Windows Internet Name Service (WINS), provides a name-resolution service for computers running NetBIOS. NetBIOS name servers maintain a database of the NetBIOS names for hosts and the corresponding IP address the host is using. NBNS aims to match IP addresses with NetBIOS names and queries. Attackers usually attack the name service first. Typically, NBNS uses UDP 137 as its transport protocol. It can also use TCP 137 as its transport protocol for a few operations, though this might never occur in practice.

- **TCP 139: NetBIOS Session Service (SMB over NetBIOS)**

  TCP 139 is perhaps the most well-known Windows port. It is used to transfer files over a network. Systems use this port for both null-session establishment as well as file and printer sharing. A system administrator considering the restriction of access to ports on a Windows system should make the restriction of TCP 139 a top priority. An improperly configured TCP 139 port can allow an intruder to gain unauthorized access to critical system files or the complete file system, resulting in data theft or other malicious activities.

- **TCP/UDP 445: SMB over TCP (Direct Host)**

  Windows supports file- and printer-sharing traffic using the SMB protocol directly hosted on TCP. In earlier OSs, SMB traffic required the NetBIOS over TCP (NBT) protocol to work on TCP/IP transport. Directly hosted SMB traffic uses port 445 (TCP and UDP) instead of NetBIOS.

- **UDP 161: Simple Network Management Protocol (SNMP)**

  SNMP is widely used in network management systems to monitor network-attached devices such as routers, switches, firewalls, printers, and servers. It consists of a manager and agents. The agent receives requests on port 161 from the managers and responds to the managers on port 162.

- **TCP/UDP 389: Lightweight Directory Access Protocol (LDAP)**

  LDAP is a protocol for accessing and maintaining distributed directory information services over an IP network. By default, LDAP uses TCP or UDP as its transport protocol over port 389.

- **TCP 2049: Network File System (NFS)**

  NFS protocol is used to mount file systems on a remote host over a network, and users can interact with the file systems as if they are mounted locally. NFS servers listen to its client systems on TCP port 2049. If NFS services are not properly configured, then attackers may exploit the NFS protocol to gain control over a remote system, perform privilege escalation, inject backdoors or malware on a remote host, etc.

- **TCP 25: Simple Mail Transfer Protocol (SMTP)**

  SMTP is a TCP/IP mail delivery protocol. It transfers email across the Internet and across local networks. It runs on the connection-oriented service provided by TCP and uses the well-known port number 25. Below table lists some commands used by SMTP and their respective syntaxes.

Hello	`HELO <sending-host>`
From	`MAIL FROM:<from-address>`
Recipient	`RCPT TO:<to-address>`
Data	`DATA`
Reset	`RESET`
Verify	`VRFY<string>`
Expand	`EXPN<string>`
Help	`HELP[string]`
Quit	`QUIT`

Table 4.1: SMTP commands and their respective syntaxes

- **TCP/UDP 162: SNMP Trap**

  An SNMP trap uses TCP/UDP port 162 to send notifications such as optional variable bindings and the sysUpTime value from an agent to a manager.

- **UDP 500: Internet Security Association and Key Management Protocol (ISAKMP)/Internet Key Exchange (IKE)**

  Internet Security Association and Key Management Protocol (ISAKMP)/Internet Key Exchange (IKE) is a protocol used to set up a security association (SA) in the IPsec protocol suite. It uses UDP port 500 to establish, negotiate, modify, and delete SAs and cryptographic keys in a virtual private network (VPN) environment.

- **TCP 22: Secure Shell (SSH)**

  Secure Shell (SSH) is a command-level protocol mainly used for managing various networked devices securely. It is generally used as an alternative protocol to the unsecure Telnet protocol. SSH uses the client/server communication model, and the SSH server, by default, listens to its client on TCP port 22. Attackers may exploit the SSH protocol by brute-forcing SSH login credentials.

- **TCP/UDP 3268: Global Catalog Service**

  Microsoft's Global Catalog server, a domain controller that stores extra information, uses port 3268. Its database contains rows for every object in the entire organization, instead of rows for only the objects in one domain. Global Catalog allows one to locate objects from any domain without having to know the domain name. LDAP in the Global Catalog server uses port 3268. This service listens to port 3268 through a TCP connection. Administrators use port 3268 for troubleshooting issues in the Global Catalog by connecting to it using LDP.

- **TCP/UDP 5060, 5061: Session Initiation Protocol (SIP)**

  The Session Initiation Protocol (SIP) is a protocol used in Internet telephony for voice and video calls. It typically uses TCP/UDP port 5060 (non-encrypted signaling traffic) or 5061 (encrypted traffic with TLS) for SIP to servers and other endpoints.

- **TCP 20/21: File Transfer Protocol**

  FTP is a connection-oriented protocol used for transferring files over the Internet and private networks. FTP is controlled on TCP port 21, and for data transmission, FTP uses TCP port 20 or some dynamic port numbers depending on the server configuration. If attackers identify that FTP server ports are open, then they perform enumeration on FTP to find information such as the software version and state of existing vulnerabilities to perform further exploitations such as the sniffing of FTP traffic and FTP brute-force attacks.

- **TCP 23: Telnet**

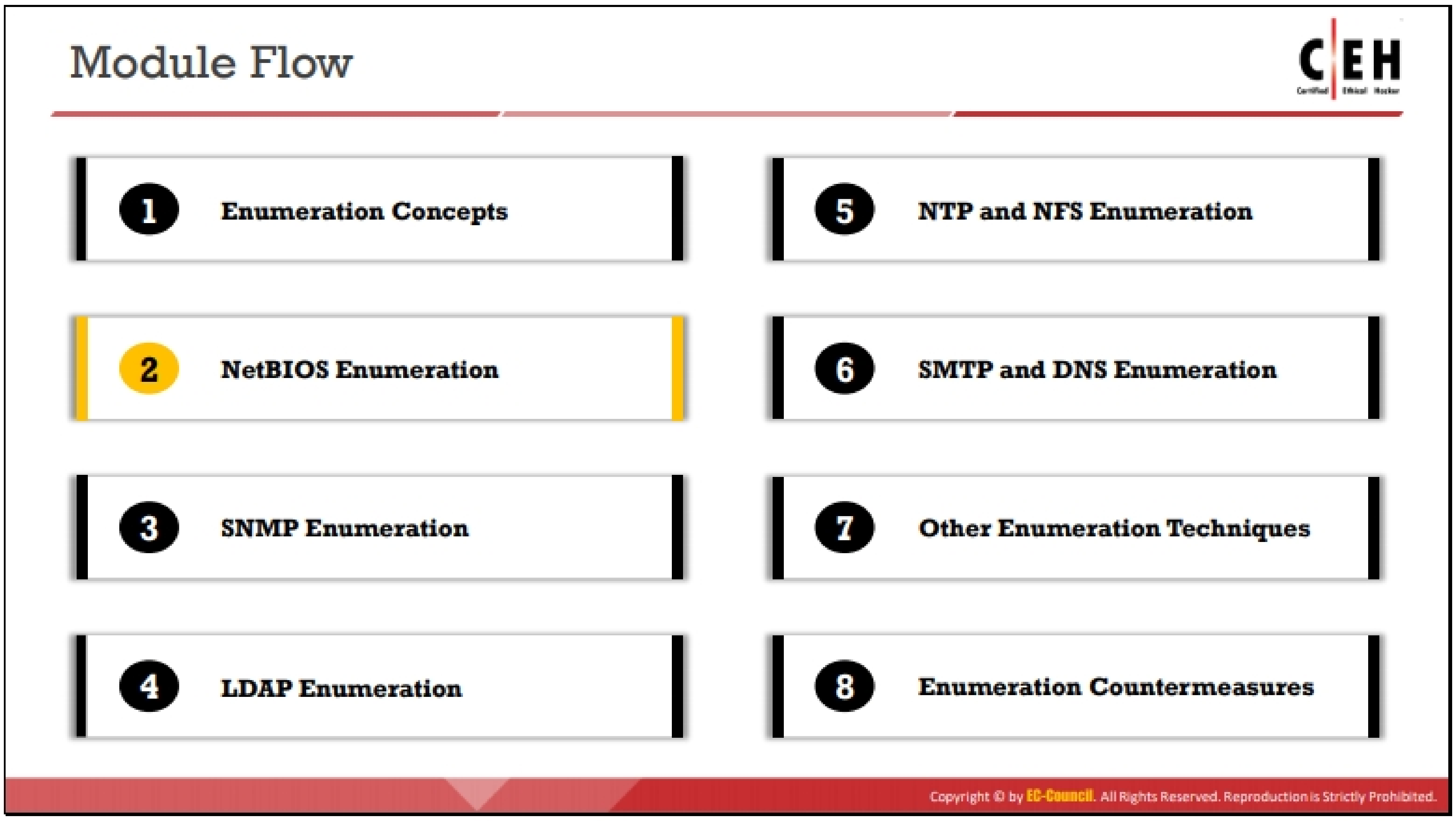
  The Telnet protocol is used for managing various networked devices remotely. It is an unsecure protocol because it transmits login credentials in the cleartext format. Therefore, it is mostly used in private networks. The Telnet server listens to its clients on port 23. Attackers can take advantage of the Telnet protocol to perform banner grabbing on other protocols such as SSH and SMTP, brute-forcing attacks on login credentials, port-forwarding attacks, etc.

- **UDP 69: Trivial File Transfer Protocol (TFTP)**

  TFTP is a connectionless protocol used for transferring files over the Internet. TFTP depends on connectionless UDP; therefore, it does not guarantee the proper transmission of the file to the destination. TFTP is mainly used to update or upgrade software and firmware on remote networked devices. It uses UDP port 69 for transferring files to a remote host. Attackers may exploit TFTP to install malicious software or firmware on remote devices.

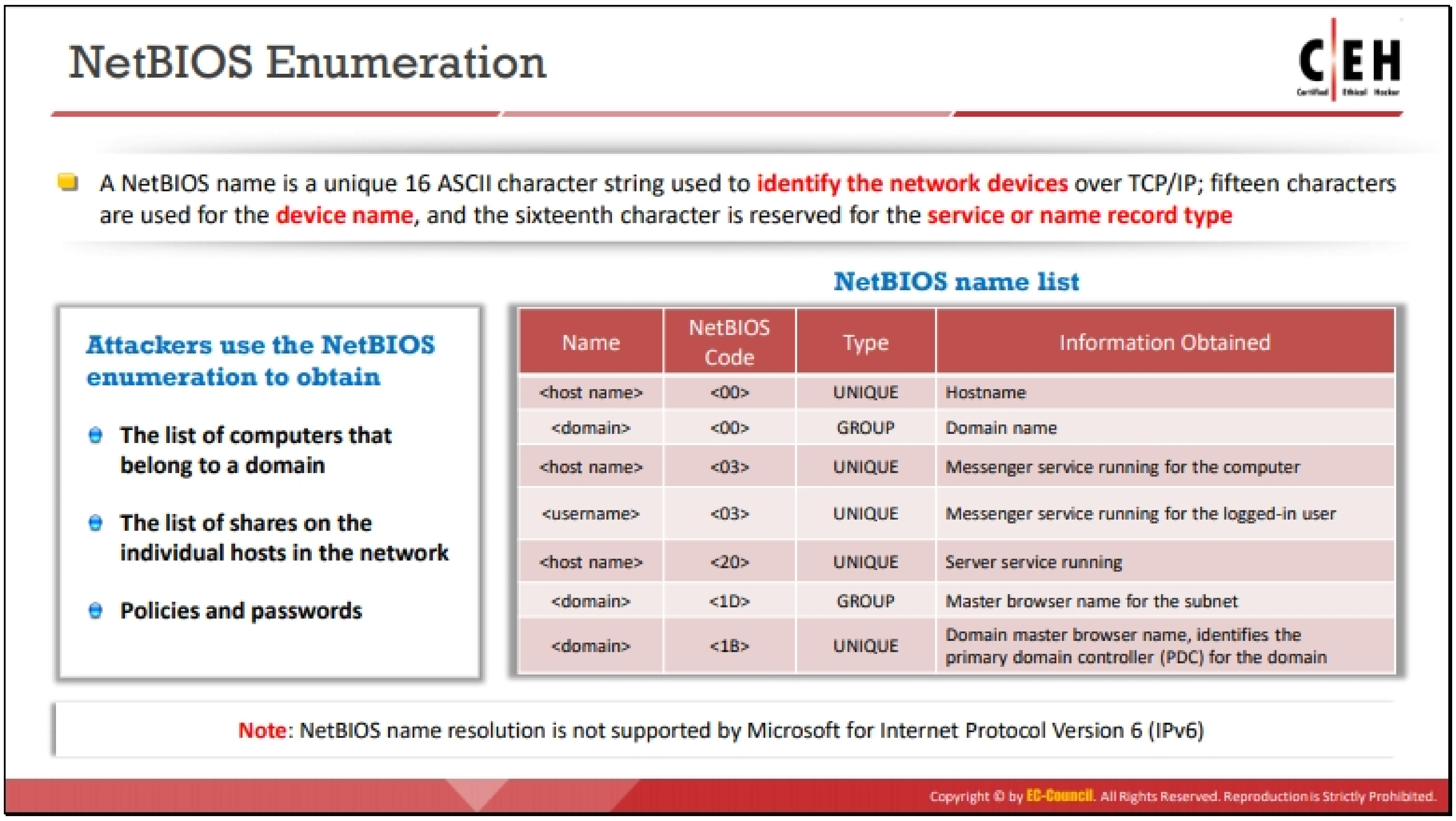
- **TCP 179: Border Gateway Protocol (BGP)**

  BGP is widely used by Internet service providers (ISPs) to maintain huge routing tables and for efficiently processing Internet traffic. BGP routers establish sessions on TCP port 179. The misconfiguration of BGP may lead to various attacks such as dictionary attacks, resource-exhaustion attacks, flooding attacks, and hijacking attacks.



Module Flow

1. **Enumeration Concepts**
2. **NetBIOS Enumeration**
3. **SNMP Enumeration**
4. **LDAP Enumeration**
5. **NTP and NFS Enumeration**
6. **SMTP and DNS Enumeration**
7. **Other Enumeration Techniques**
8. **Enumeration Countermeasures**



NetBIOS Enumeration

- A NetBIOS name is a unique 16 ASCII character string used to **identify the network devices** over TCP/IP; fifteen characters are used for the **device name**, and the sixteenth character is reserved for the **service or name record type**

Attackers use the NetBIOS enumeration to obtain

- **The list of computers that belong to a domain**
- **The list of shares on the individual hosts in the network**
- **Policies and passwords**

NetBIOS name list

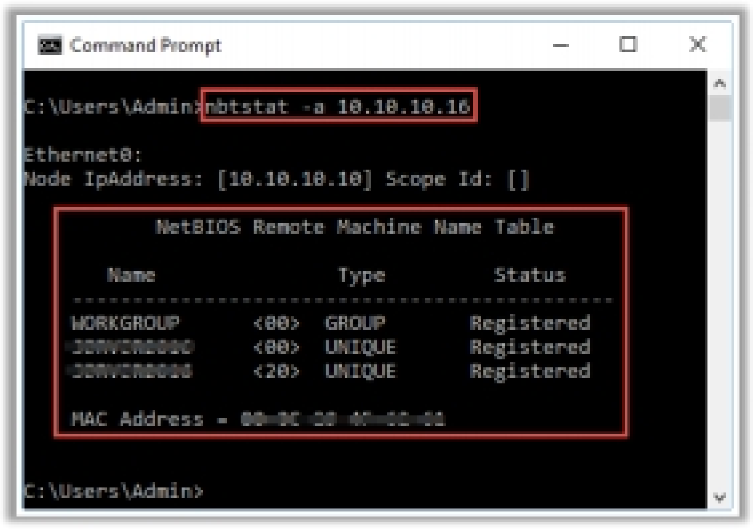
Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for the computer
<username>	<03>	UNIQUE	Messenger service running for the logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the primary domain controller (PDC) for the domain

Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

NetBIOS Enumeration (Cont'd)

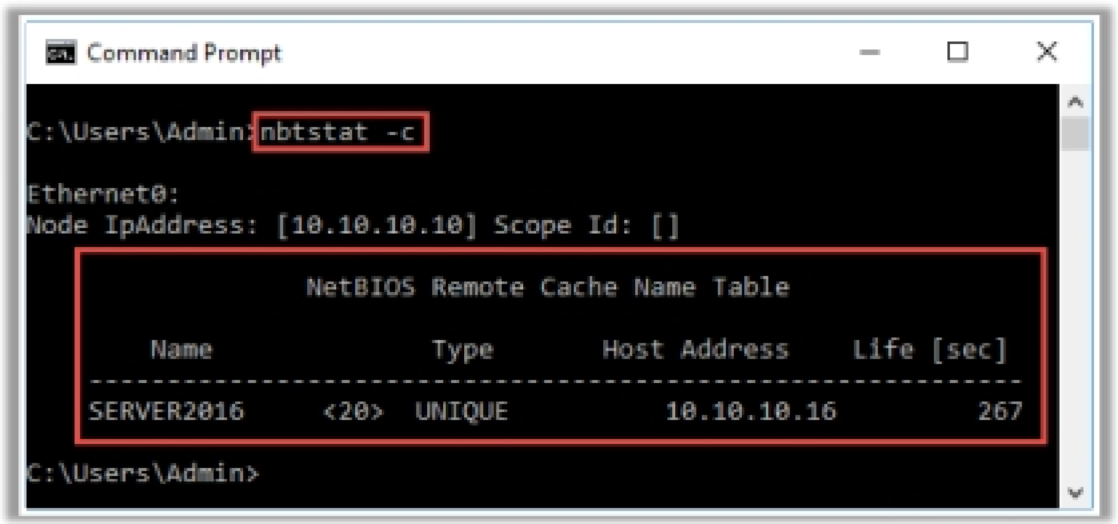
- The nbtstat utility in Windows displays NetBIOS over **TCP/IP** (NetBT) **protocol statistics**, **NetBIOS name tables** for both the local and remote computers, and the **NetBIOS name cache**

- Run the **`nbtstat`** command "**`nbtstat -a <IP address of the remote machine>`**" to obtain the NetBIOS name table of a remote computer



```
C:\Users\Admin>nbtstat -a 10.10.10.16

Ethernet0:
Node IpAddress: [10.10.10.10] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WORKGROUP      <00>  GROUP       Registered
    [redacted]     <00>  UNIQUE      Registered
    [redacted]     <20>  UNIQUE      Registered

    MAC Address = [redacted]

C:\Users\Admin>
```

- Run the **`nbtstat`** command "**`nbtstat -c`**" to obtain the contents of the NetBIOS name cache, table of NetBIOS names, and their resolved IP addresses



```
C:\Users\Admin>nbtstat -c

Ethernet0:
Node IpAddress: [10.10.10.10] Scope Id: []

                  NetBIOS Remote Cache Name Table

        Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    SERVER2016     <20>  UNIQUE          10.10.10.16         267

C:\Users\Admin>
```

https://docs.microsoft.com

NetBIOS Enumeration

Thus far, we discussed enumeration concepts and resources that provide valuable information. This section describes NetBIOS enumeration, the information obtained, and various NetBIOS enumeration tools. NetBIOS is considered first for enumeration because it extracts a large amount of sensitive information about the target network, such as users and network shares.

The first step in enumerating a Windows system is to take advantage of the NetBIOS API. NetBIOS was originally developed as an API for client software to access local area network (LAN) resources. Windows uses NetBIOS for file and printer sharing. The NetBIOS name is a unique 16-character ASCII string assigned to Windows systems to identify network devices over TCP/IP; 15 characters are used for the device name, and the 16th is reserved for the service or record type. NetBIOS uses UDP port 137 (name services), UDP port 138 (datagram services), and TCP port 139 (session services). Attackers usually target the NetBIOS service because it is easy to exploit and run on Windows systems even when not in use.

Attackers use NetBIOS enumeration to obtain the following:

- The list of computers that belong to a domain
- The list of shares on the individual hosts in a network
- Policies and passwords

An attacker who finds a Windows system with port 139 open can check to see which resources can be accessed or viewed on a remote system. However, to enumerate the NetBIOS names, the remote system must have enabled file and printer sharing. NetBIOS enumeration may enable an attacker to read or write to a remote computer system, depending on the availability of shares, or launch a DoS attack.

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for the computer
<username>	<03>	UNIQUE	Messenger service running for the logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, which identifies the primary domain controller (PDC) for the domain
<domain>	<1E>	GROUP	Browser service elections

Table 4.2: NetBIOS name list

Note that Microsoft does not support NetBIOS name resolution for IPv6.

Nbtstat Utility

Source: *https://docs.microsoft.com*

Nbtstat is a Windows utility that helps in troubleshooting NETBIOS name resolution problems. The `nbtstat` command removes and corrects preloaded entries using several case-sensitive switches. Attackers use Nbtstat to enumerate information such as NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both local and remote computers, and the NetBIOS name cache.

The syntax of the nbtstat command is as follows:

```
nbtstat [-a RemoteName] [-A IP Address] [-c] [-n] [-r] [-R] [-RR] [-s]
[-S] [Interval]
```

The table shown below lists various Nbtstat parameters and their respective functions.

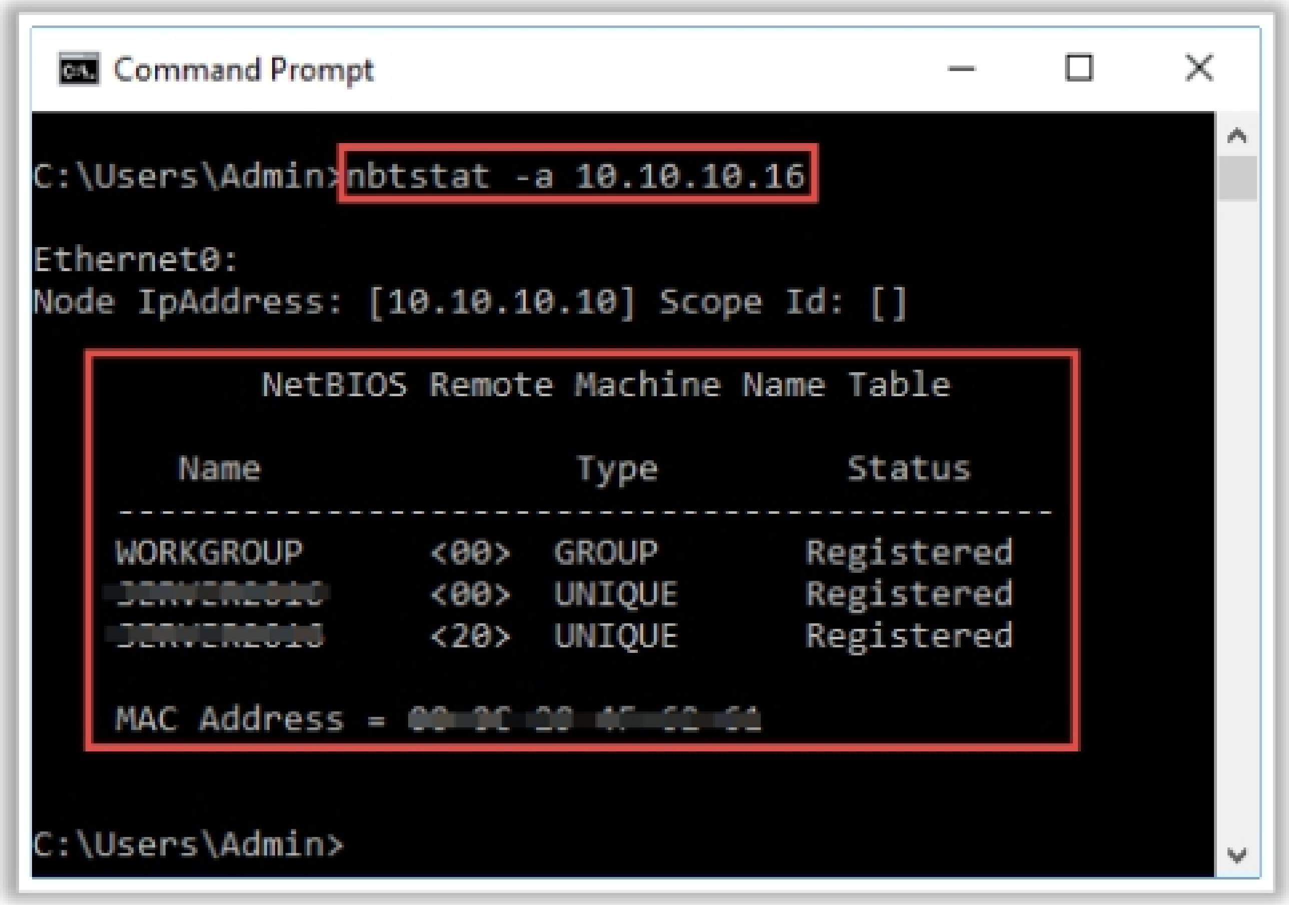
Nbtstat Parameter	Function
`-a RemoteName`	Displays the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer
`-A IP Address`	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer
`-c`	Lists the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses
`-n`	Displays the names registered locally by NetBIOS applications such as the server and redirector
`-r`	Displays a count of all names resolved by a broadcast or WINS server

`-R`	Purges the name cache and reloads all #PRE-tagged entries from the Lmhosts file
`-RR`	Releases and re-registers all names with the name server
`-s`	Lists the NetBIOS sessions table converting destination IP addresses to computer NetBIOS names
`-S`	Lists the current NetBIOS sessions and their status with the IP addresses
`Interval`	Re-displays selected statistics, pausing at each display for the number of seconds specified in Interval

Table 4.3: Nbtstat parameters and their respective functions

The following are some examples for nbtstat commands.

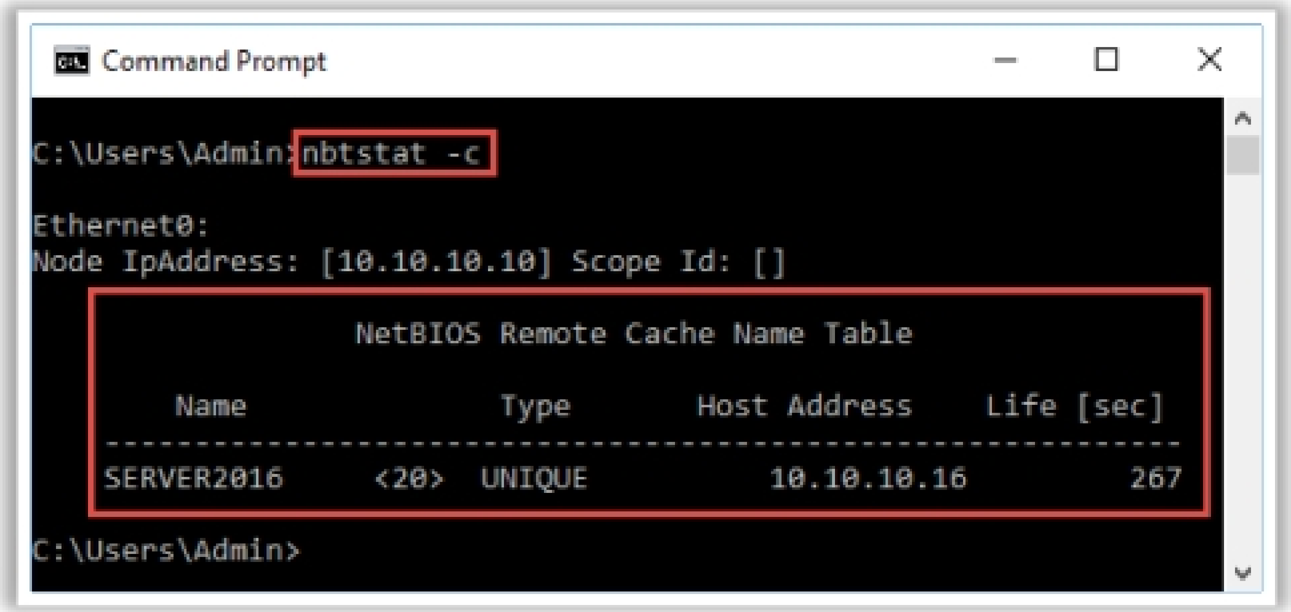
- The nbtstat command "**`nbtstat -a <IP address of the remote machine>`**" can be executed to obtain the NetBIOS name table of a remote computer.



```
C:\Users\Admin>nbtstat -a 10.10.10.16

Ethernet0:
Node IpAddress: [10.10.10.10] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WORKGROUP      <00>  GROUP       Registered
    [redacted]     <00>  UNIQUE      Registered
    [redacted]     <20>  UNIQUE      Registered

    MAC Address = [redacted]


C:\Users\Admin>
```

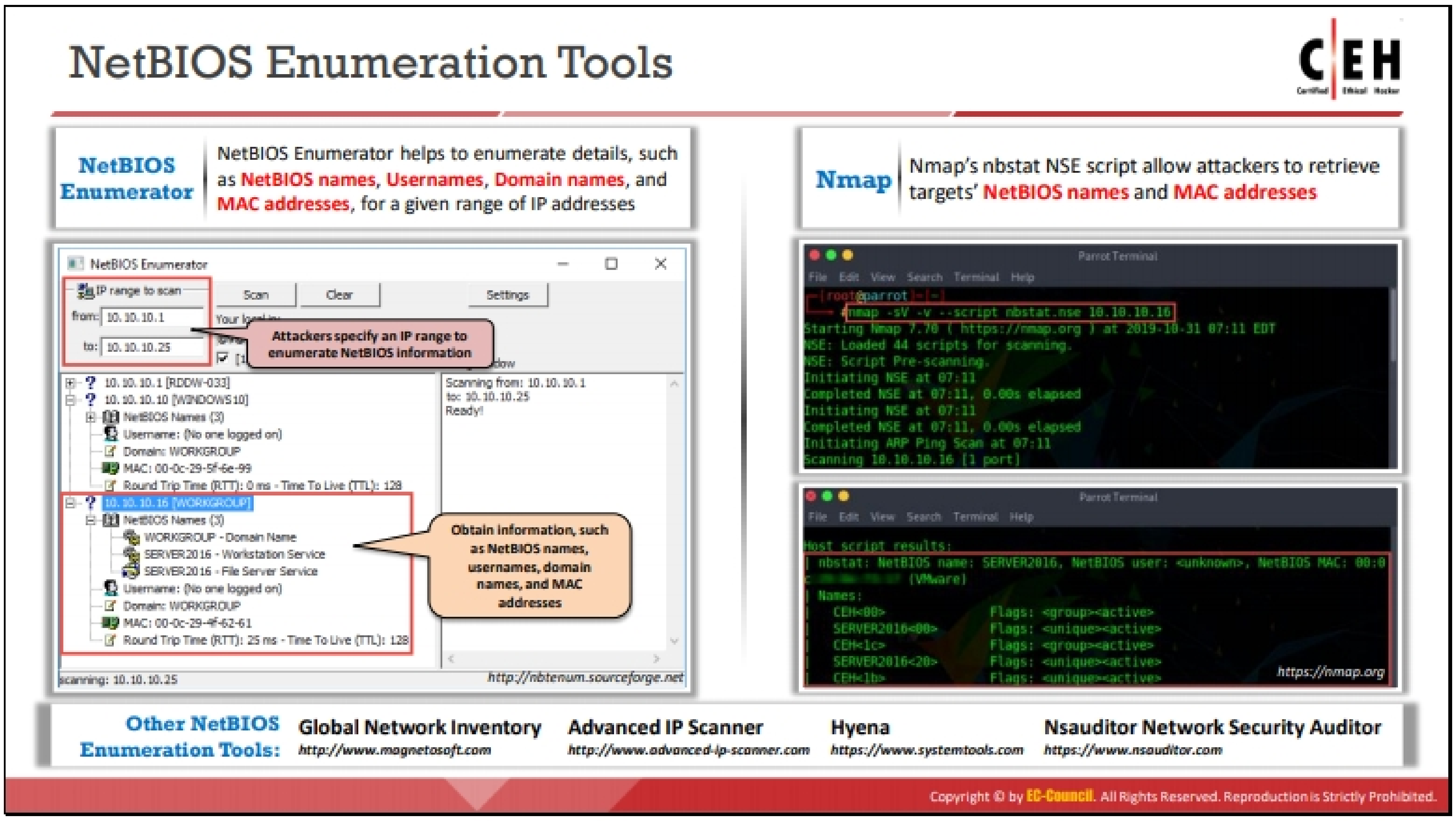
Figure 4.1: Nbtstat command to obtain the name table of a remote system

- The nbtstat command "**`nbtstat -c`**" can be executed to obtain the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.



```
C:\Users\Admin>nbtstat -c

Ethernet0:
Node IpAddress: [10.10.10.10] Scope Id: []

                  NetBIOS Remote Cache Name Table

        Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    SERVER2016     <20>  UNIQUE          10.10.10.16         267

C:\Users\Admin>
```

Figure 4.2: Nbtstat command to obtain the contents of the NetBIOS name table



NetBIOS Enumeration Tools

NetBIOS Enumerator NetBIOS Enumerator helps to enumerate details, such as **NetBIOS names**, **Usernames**, **Domain names**, and **MAC addresses**, for a given range of IP addresses

from: 10.10.10.1
to: 10.10.10.25

Attackers specify an IP range to enumerate NetBIOS information

```
10.10.10.1 [RDDW-033]
10.10.10.10 [WINDOWS10]
    NetBIOS Names (3)
    Username: (No one logged on)
    Domain: WORKGROUP
    MAC: 00-0c-29-5f-6e-99
    Round Trip Time (RTT): 0 ms - Time To Live (TTL): 128
10.10.10.16 [WORKGROUP]
    NetBIOS Names (3)
        WORKGROUP - Domain Name
        SERVER2016 - Workstation Service
        SERVER2016 - File Server Service
    Username: (No one logged on)
    Domain: WORKGROUP
    MAC: 00-0c-29-4f-62-61
    Round Trip Time (RTT): 25 ms - Time To Live (TTL): 128
```

```
Scanning from: 10.10.10.1
to: 10.10.10.25
Ready!
```

```
scanning: 10.10.10.25
```

Obtain information, such as NetBIOS names, usernames, domain names, and MAC addresses

http://nbtenum.sourceforge.net

Nmap Nmap's nbstat NSE script allow attackers to retrieve targets' **NetBIOS names** and **MAC addresses**

```
┌─[root@parrot]─[~]
└──╼ #nmap -sV -v --script nbstat.nse 10.10.10.16
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-31 07:11 EDT
NSE: Loaded 44 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:11
Completed NSE at 07:11, 0.00s elapsed
Initiating NSE at 07:11
Completed NSE at 07:11, 0.00s elapsed
Initiating ARP Ping Scan at 07:11
Scanning 10.10.10.16 [1 port]
```

```
Host script results:
| nbstat: NetBIOS name: SERVER2016, NetBIOS user: <unknown>, NetBIOS MAC: 00:0
c[redacted] (VMware)
| Names:
|   CEH<00>              Flags: <group><active>
|   SERVER2016<00>       Flags: <unique><active>
|   CEH<1c>              Flags: <group><active>
|   SERVER2016<20>       Flags: <unique><active>
|   CEH<1b>              Flags: <unique><active>
```

https://nmap.org

Other NetBIOS Enumeration Tools:

- **Global Network Inventory** *http://www.magnetosoft.com*
- **Advanced IP Scanner** *http://www.advanced-ip-scanner.com*
- **Hyena** *https://www.systemtools.com*
- **Nsauditor Network Security Auditor** *https://www.nsauditor.com*

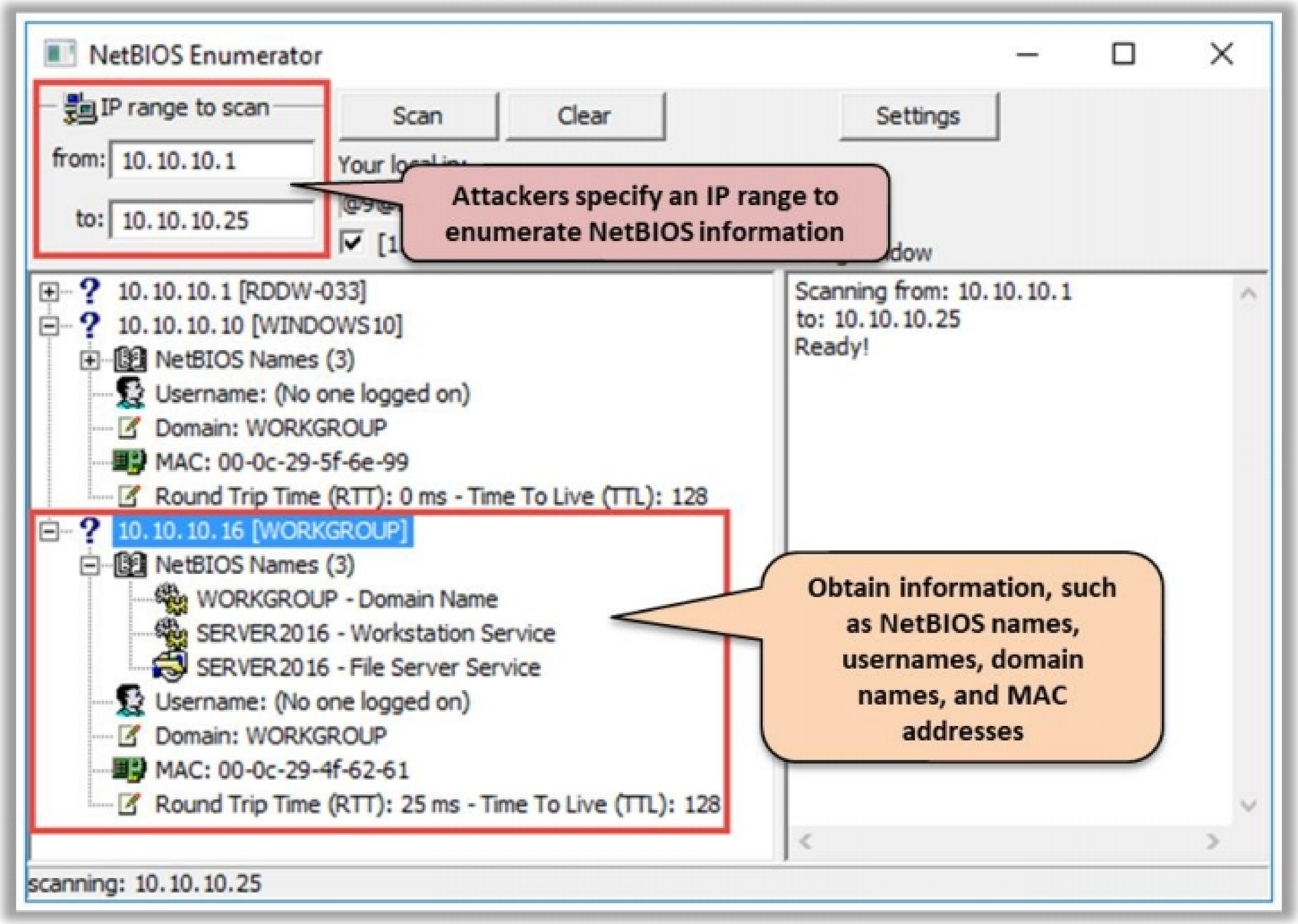
NetBIOS Enumeration Tools

NetBIOS enumeration tools explore and scan a network within a given range of IP addresses and lists of computers to identify security loopholes or flaws in networked systems. These tools also enumerate operating systems (OSs), users, groups, Security Identifiers (SIDs), password policies, services, service packs and hotfixes, NetBIOS shares, transports, sessions, disks and security event logs, etc.

- **NetBIOS Enumerator**

  Source: *http://nbtenum.sourceforge.net*

  NetBIOS Enumerator is an enumeration tool that shows how to use remote network support and to deal with some other web protocols, such as SMB. As shown in the screenshot, attackers use NetBIOS Enumerator to enumerate details such as NetBIOS names, usernames, domain names, and media access control (MAC) addresses for a given range of IP addresses.



from: 10.10.10.1
to: 10.10.10.25

Attackers specify an IP range to enumerate NetBIOS information

```
10.10.10.1 [RDDW-033]
10.10.10.10 [WINDOWS10]
    NetBIOS Names (3)
    Username: (No one logged on)
    Domain: WORKGROUP
    MAC: 00-0c-29-5f-6e-99
    Round Trip Time (RTT): 0 ms - Time To Live (TTL): 128
10.10.10.16 [WORKGROUP]
    NetBIOS Names (3)
        WORKGROUP - Domain Name
        SERVER2016 - Workstation Service
        SERVER2016 - File Server Service
    Username: (No one logged on)
    Domain: WORKGROUP
    MAC: 00-0c-29-4f-62-61
    Round Trip Time (RTT): 25 ms - Time To Live (TTL): 128
```

```
Scanning from: 10.10.10.1
to: 10.10.10.25
Ready!
```

Obtain information, such as NetBIOS names, usernames, domain names, and MAC addresses

```
scanning: 10.10.10.25
```

Figure 4.3: Screenshot of NetBIOS Enumerator

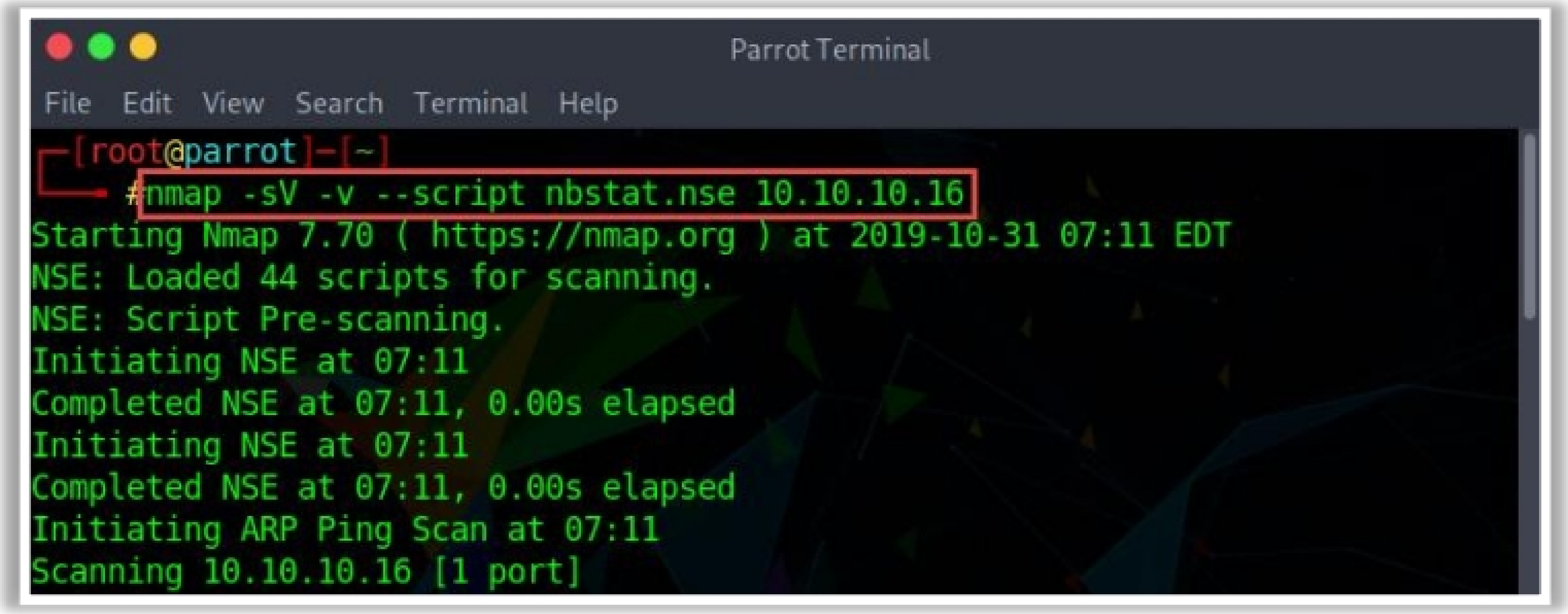
- **Nmap**

  Source: *https://nmap.org*

  Attackers use the Nmap Scripting Engine (NSE) for discovering NetBIOS shares on a network. The nbstat script of NSE allows attackers to retrieve the target's NetBIOS names and MAC addresses. By default, the script displays the name of the computer and the logged-in user. However, if the verbosity is turned up, it displays all names related to that system.

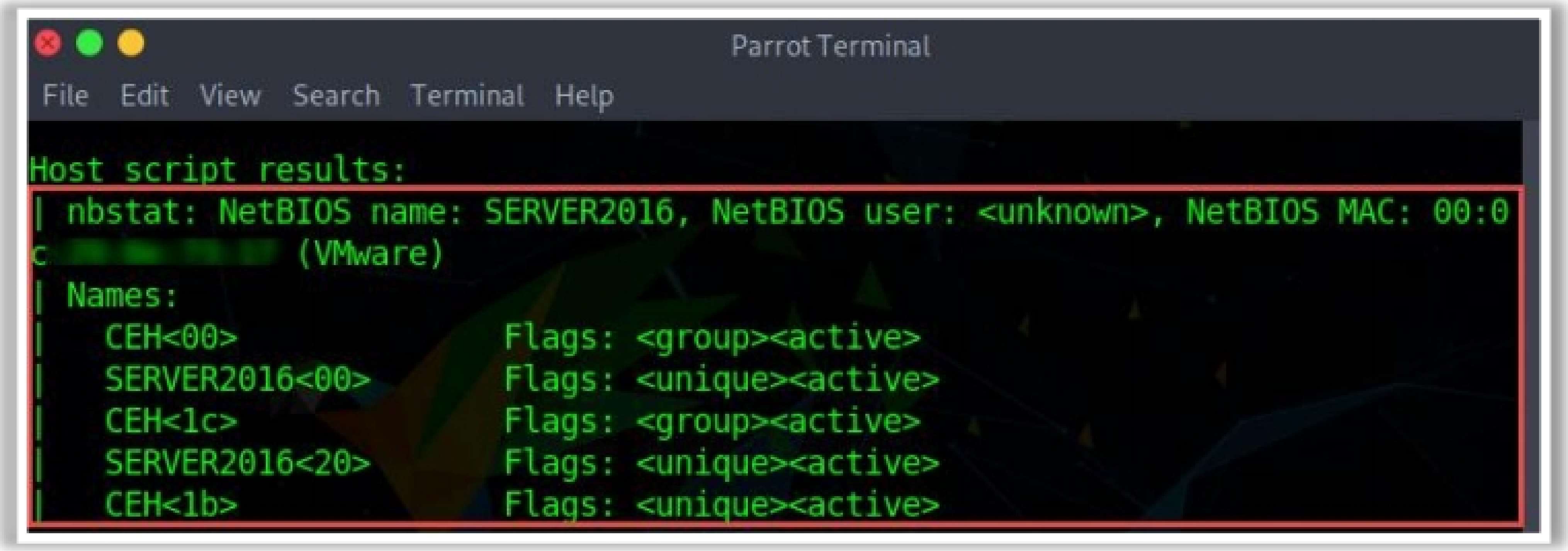
  As shown in the screenshot, an attacker uses the following Nmap command to perform NetBIOS enumeration on a target host:

  ```
  nmap -sV -v --script nbstat.nse <target IP address>
  ```



```
┌─[root@parrot]─[~]
└──╼ #nmap -sV -v --script nbstat.nse 10.10.10.16
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-31 07:11 EDT
NSE: Loaded 44 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:11
Completed NSE at 07:11, 0.00s elapsed
Initiating NSE at 07:11
Completed NSE at 07:11, 0.00s elapsed
Initiating ARP Ping Scan at 07:11
Scanning 10.10.10.16 [1 port]
```

Figure 4.4: Screenshot of Nmap command for NetBIOS enumeration

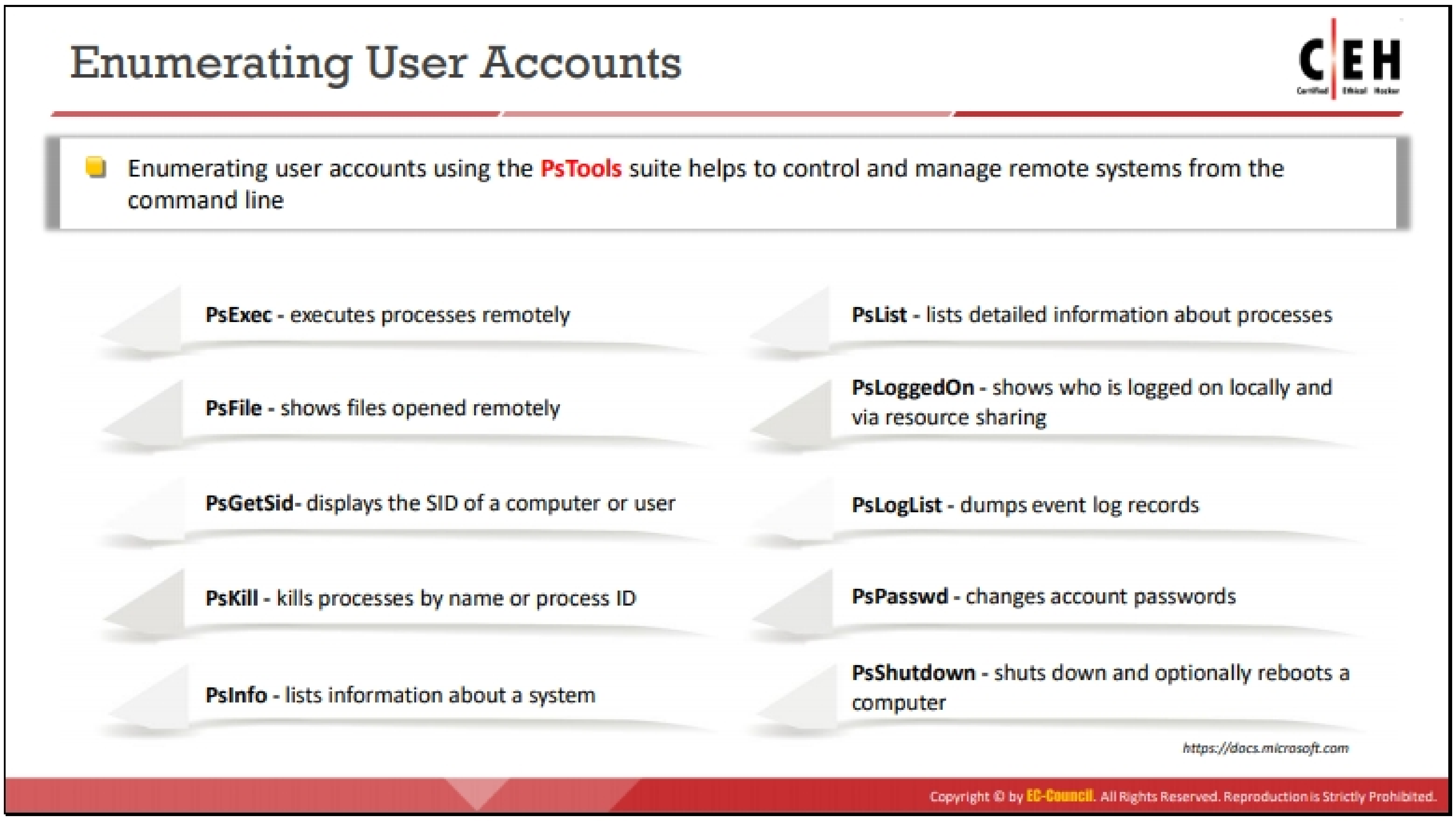


```
Host script results:
| nbstat: NetBIOS name: SERVER2016, NetBIOS user: <unknown>, NetBIOS MAC: 00:0
c[redacted] (VMware)
| Names:
|   CEH<00>              Flags: <group><active>
|   SERVER2016<00>       Flags: <unique><active>
|   CEH<1c>              Flags: <group><active>
|   SERVER2016<20>       Flags: <unique><active>
|   CEH<1b>              Flags: <unique><active>
```

Figure 4.5: Screenshot of Nmap NetBIOS enumeration output

The following are some additional NetBIOS enumeration tools:

- Global Network Inventory (*http://www.magnetosoft.com*)
- Advanced IP Scanner (*http://www.advanced-ip-scanner.com*)
- Hyena (*https://www.systemtools.com*)
- Nsauditor Network Security Auditor (*https://www.nsauditor.com*)



Enumerating User Accounts

- Enumerating user accounts using the **PsTools** suite helps to control and manage remote systems from the command line

PsExec - executes processes remotely

PsFile - shows files opened remotely

PsGetSid- displays the SID of a computer or user

PsKill - kills processes by name or process ID

PsInfo - lists information about a system

PsList - lists detailed information about processes

PsLoggedOn - shows who is logged on locally and via resource sharing

PsLogList - dumps event log records

PsPasswd - changes account passwords

PsShutdown - shuts down and optionally reboots a computer

https://docs.microsoft.com

Enumerating User Accounts

Source: *https://docs.microsoft.com*

Enumerating user accounts using the PsTools suite helps in controlling and managing remote systems from the command line. The following are some commands for enumerating user accounts.

- **PsExec**

  PsExec is a lightweight Telnet replacement that can execute processes on other systems, complete with full interactivity for console applications, without having to install client software manually. PsExec's most powerful use case is the launch of interactive command prompts on remote systems and remote-enabling tools such as Ipconfig that otherwise cannot show information about remote systems. The syntax of the PsExec command is as follows:

  ```
  psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd][-n s][-r servicename][-h][-l][-s|-e][-x][-I [session]][-c [-f|-v]][-w directory][-d][-<priority>][-a n,n,...] cmd [arguments]
  ```

- **PsFile**

  PsFile is a command-line utility that shows a list of files on a system that opened remotely, and it can close opened files either by name or by a file identifier. The default behavior of PsFile is to list the files on the local system opened by remote systems. Typing a command followed by "- " displays information on the syntax for that command. The syntax of the PsFile command is as follows:

  ```
  psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id | path] [-c]]
  ```

- **PsGetSid**

  PsGetSid translates SIDs to their display name and vice versa. It works on built-in accounts, domain accounts, and local accounts. It also displays the SIDs of user accounts and translates an SID into the name that represents it. It works across the network to query SIDs remotely. The syntax of the PsGetSid command is as follows:

  ```
  psgetsid [\\computer[,computer[,...] | @file] [-u username [-p password]]] [account|SID]
  ```

- **PsKill**

  PsKill is a kill utility that can kill processes on remote systems and terminate processes on the local computer. Running PsKill with a process ID directs it to kill the process of that ID on the local computer. If a process name is specified, PsKill will kill all processes that have that name. One need not install a client on the target computer to use PsKill to terminate a remote process. The syntax of the PsKill command is as follows:

  ```
  pskill [- ] [-t] [\\computer [-u username] [-p password]] <process name | process id>
  ```

- **PsInfo**

  PsInfo is a command-line tool that gathers key information about local or remote legacy Windows NT/2000 systems, including the type of installation, kernel build, registered organization and owner, number of processors and their type, amount of physical memory, installation date of the system, and expiration date in the case of a trial version. By default, PsInfo shows information for the local system. A remote computer name can be specified to obtain information for a remote system. The syntax of the PsInfo command is as follows:

  ```
  psinfo [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] [-h] [-s] [-d] [-c [-t delimiter]] [filter]
  ```

- **PsList**

  PsList is a command-line tool that displays central processing unit (CPU) and memory information or thread statistics. Tools in the Resource Kits, pstat and pmon, show different types of data only for the processes on the system on which the tools are run.

- **PsLoggedOn**

  PsLoggedOn is an applet that displays both the locally logged-in users and users logged in via resources for either the local computer or a remote one. If a username is specified instead of a computer, PsLoggedOn searches the computers in the network neighborhood and reveals if the user currently logged in. PsLoggedOn defines a locally logged-in user is one that has a profile loaded into the registry. Therefore, PsLoggedOn determines who is logged in by scanning the keys under the HKEY_USERS key. For each key that has a name or user SID, PsLoggedOn looks up the corresponding username and displays it. To determine who logged into a computer via resource shares, PsLoggedOn uses the NetSessionEnum API. The syntax of the PsLoggedOn command is as follows:

  ```
  psloggedon [- ] [-l] [-x] [\\computername | username]
  ```

- **PsLogList**

  The elogdump utility dumps the contents of an Event Log on a local or remote computer. PsLogList is a clone of elogdump except that PsLogList can log in to remote systems in situations where the user's security credentials would not permit access to the Event Log, and PsLogList retrieves message strings from the computer on which the event log is stored. The default function of PsLogList is to display the contents of the System Event Log on the local computer with visually friendly formatting. The syntax of the PsLogList command is as follows:

```
psloglist [- ] [\\computer[,computer[,...] | @file [-u username [-
p password]]] [-s [-t delimiter]] [-m #|-n #|-h #|-d #|-w][-c][-
x][-r][-a mm/dd/yy][-b mm/dd/yy][-f filter] [-i ID[,ID[,...] | -e
ID[,ID[,...]]] [-o event source[,event source][,..]]] [-q event
source[,event source][,..]]] [-l event log file] <eventlog>
```

- **PsPasswd**

  PsPasswd can change an account password on local or remote systems, and administrators can create batch files that run PsPasswd on the computers they manage to perform a mass change of the administrator password. PsPasswd uses Windows password reset APIs; therefore, it does not send passwords over the network in the cleartext. The syntax of the PsPasswd command is as follows:

```
pspasswd [[\\computer[,computer[,..] | @file [-u user [-p psswd]]]
Username [NewPassword]
```

- **PsShutdown**

  PsShutdown can shut down or reboot a local or remote computer. It requires no manual installation of client software. The syntax of the PsShutdown command is as follows:

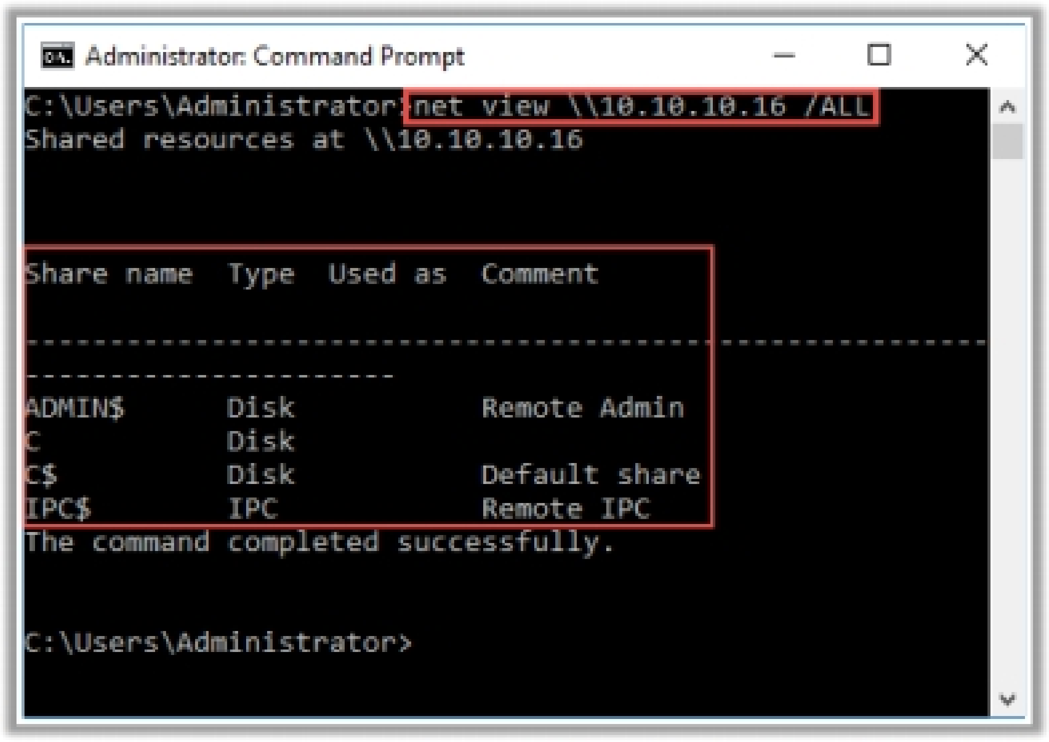
```
psshutdown [[\\computer[,computer[,..] | @file [-u user [-p
psswd]]] -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t nn|h:m] [-n s] [-v
nn] [-e [u|p]:xx:yy] [-m "message"]
```

Enumerating Shared Resources Using Net View

- The Net View utility is used to obtain a list of all the **shared resources of a remote host** or **workgroup**

Net View Commands

- **net view \\<computername>**
- **net view /domain:<domain name>**



```
C:\Users\Administrator>net view \\10.10.10.16 /ALL
Shared resources at \\10.10.10.16



Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
ADMIN$      Disk           Remote Admin
C           Disk
C$          Disk           Default share
IPC$        IPC            Remote IPC
The command completed successfully.


C:\Users\Administrator>
```

Enumerating Shared Resources Using Net View

Net View is a command-line utility that displays a list of computers in a specified workgroup or shared resources available on a specified computer. It can be used in the following ways.

`net view \\<computername>`

In the above command, `<computername>` is the name or IP address of a specific computer, the resources of which are to be displayed.

`net view \\<computername> /ALL`

The above command displays all the shares on the specified remote computer, along with hidden shares.

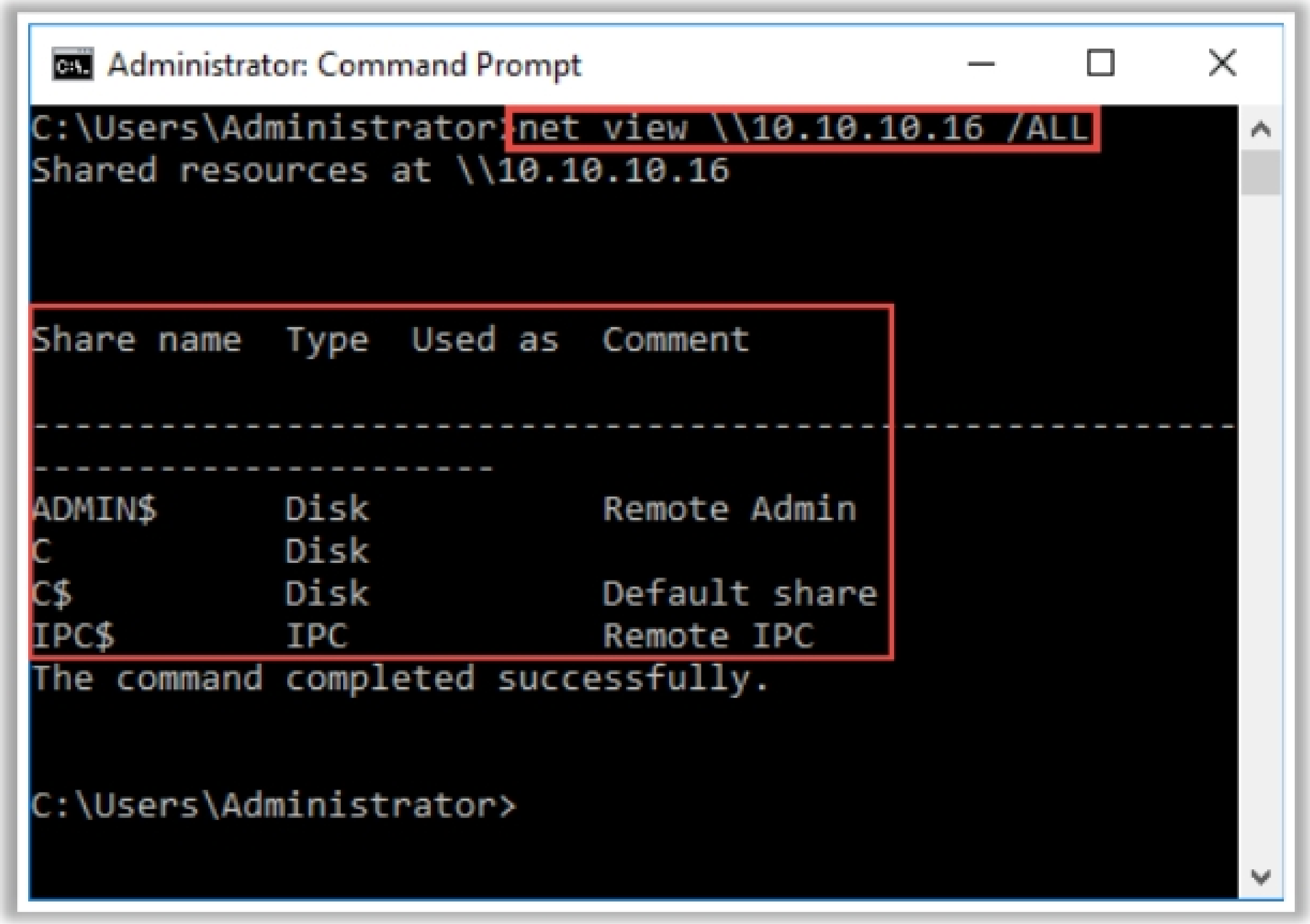
`net view /domain`

The above command displays all the shares in the domain.

`net view /domain:<domain name>`

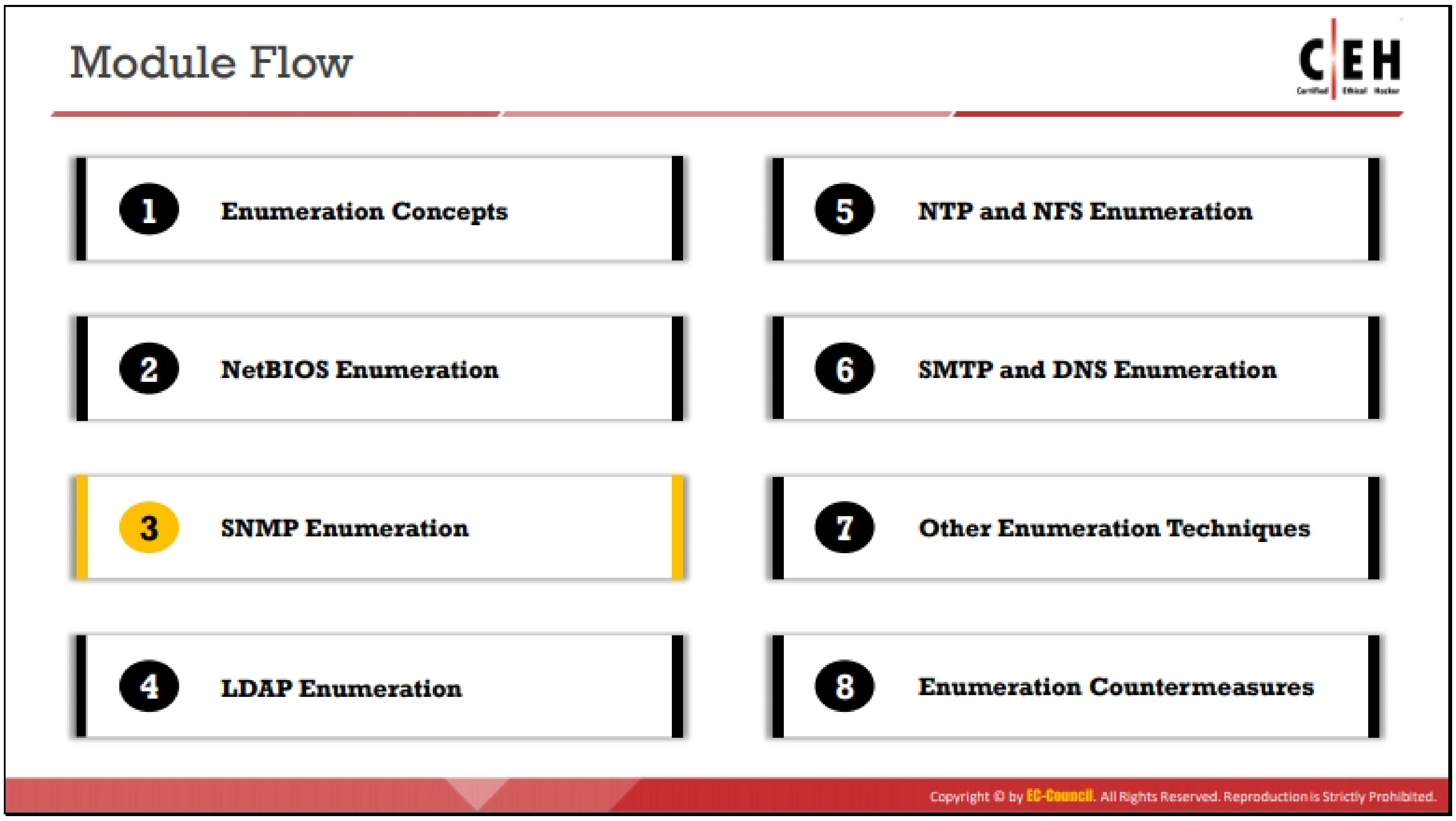
The above command displays all the shares on the specified domain.

The screenshot shows the shared resources available on the specified computer.



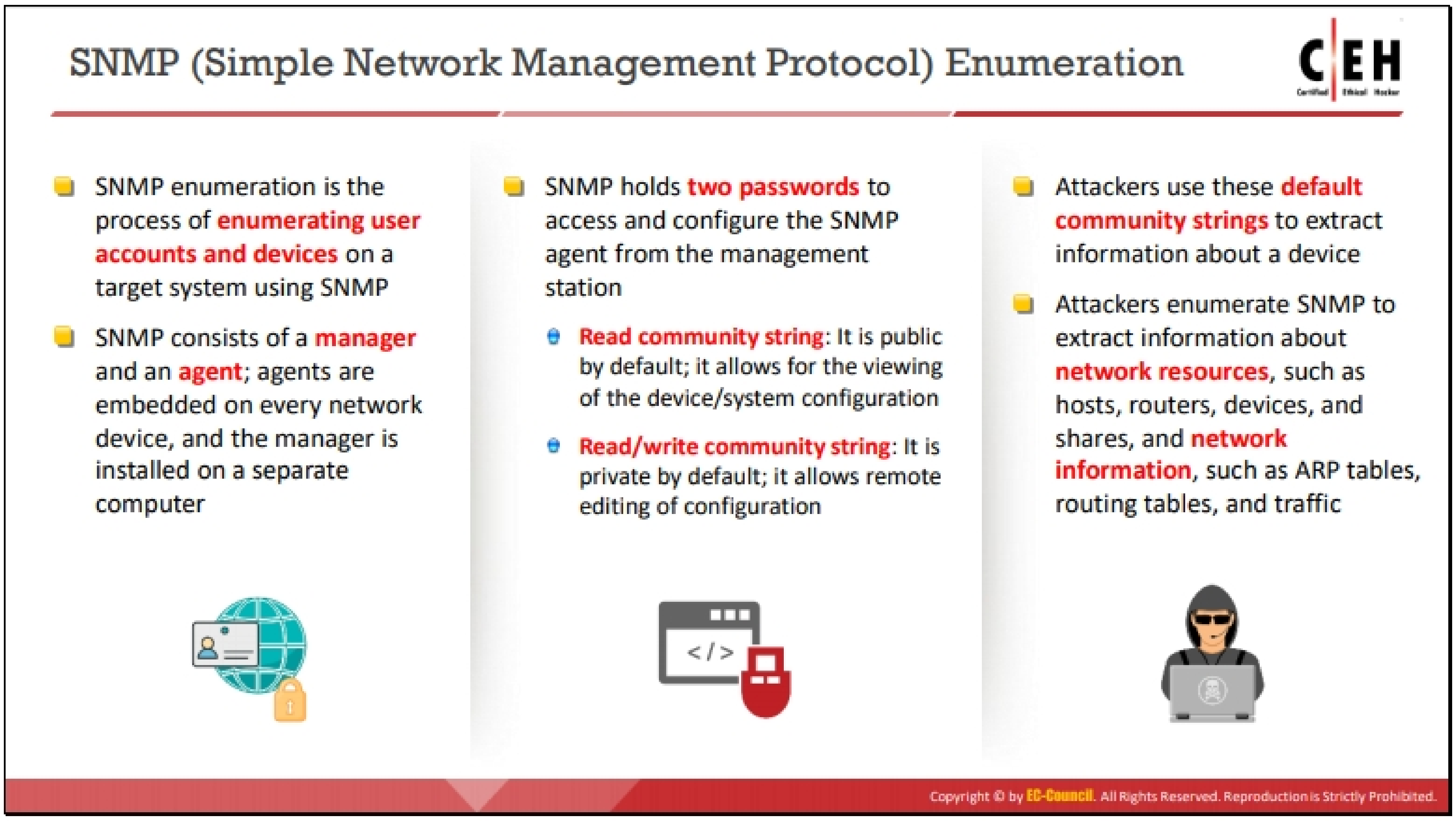
```
C:\Users\Administrator>net view \\10.10.10.16 /ALL
Shared resources at \\10.10.10.16



Share name  Type  Used as  Comment


-------------------------------------------------------------------------------
ADMIN$      Disk           Remote Admin
C           Disk
C$          Disk           Default share
IPC$        IPC            Remote IPC
The command completed successfully.


C:\Users\Administrator>
```

Figure 4.6: Output of Net View command



Module Flow

1. **Enumeration Concepts**
2. **NetBIOS Enumeration**
3. **SNMP Enumeration**
4. **LDAP Enumeration**
5. **NTP and NFS Enumeration**
6. **SMTP and DNS Enumeration**
7. **Other Enumeration Techniques**
8. **Enumeration Countermeasures**



SNMP (Simple Network Management Protocol) Enumeration

- SNMP enumeration is the process of **enumerating user accounts and devices** on a target system using SNMP
- SNMP consists of a **manager** and an **agent**; agents are embedded on every network device, and the manager is installed on a separate computer

- SNMP holds **two passwords** to access and configure the SNMP agent from the management station
  - **Read community string**: It is public by default; it allows for the viewing of the device/system configuration
  - **Read/write community string**: It is private by default; it allows remote editing of configuration

- Attackers use these **default community strings** to extract information about a device
- Attackers enumerate SNMP to extract information about **network resources**, such as hosts, routers, devices, and shares, and **network information**, such as ARP tables, routing tables, and traffic

SNMP Enumeration

SNMP allows network administrators to manage network devices from a remote location. However, SNMP has many security vulnerabilities, such as a lack of auditing. Attackers may take advantage of these vulnerabilities to perform account and device enumeration. This section describes SNMP enumeration, the information extracted via SNMP enumeration, and various SNMP enumeration tools used to enumerate user accounts and devices on a target system.

SNMP is an application-layer protocol that runs on UDP and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on Windows and Unix networks on networking devices.

SNMP enumeration is the process of creating a list of the user's accounts and devices on a target computer using SNMP. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

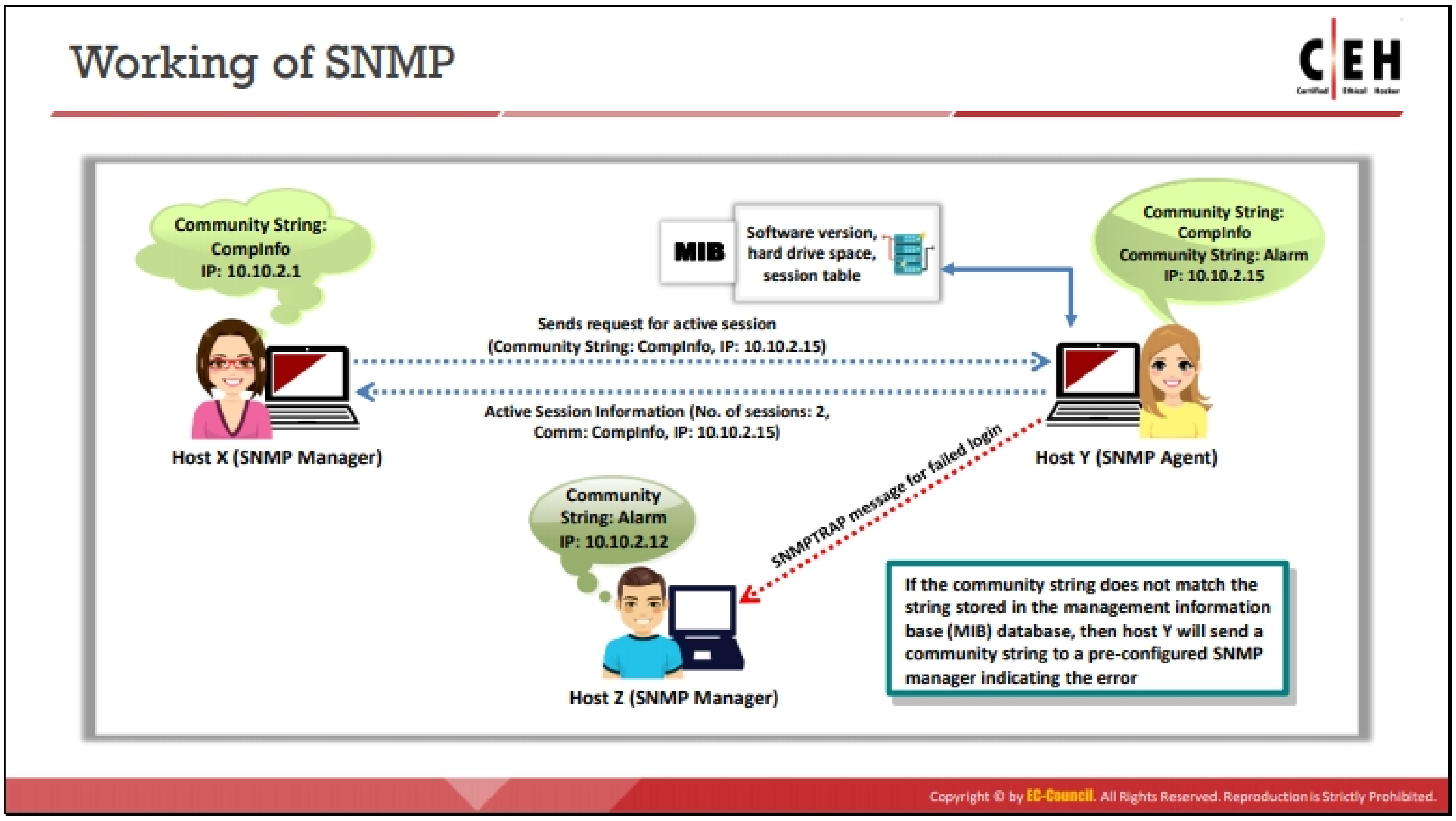
Almost all the network infrastructure devices such as routers and switches contain an SNMP agent for managing the system or devices. The SNMP management station sends requests to the agent; after receiving the request, the agent replies. Both requests and replies are configuration variables accessible by the agent software. SNMP management stations send requests to set values to some variables. Traps let the management station know if an abnormal event such as a reboot or an interface failure has occurred at the agent's side.

SNMP contains the following two passwords for configuring and accessing the SNMP agent from the management station.

- **Read Community String**
    - The configuration of the device or system can be viewed with the help of this password.
    - These strings are public.
- **Read/Write Community String**
    - The device configuration can be changed or edited using this password.
    - These strings are private.

When administrators leave the community strings at the default setting, attackers can use these default community strings (passwords) for changing or viewing the configuration of the device or system. Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, and shares as well as network information such as ARP tables, routing tables, device-specific information, and traffic statistics.

Commonly used SNMP enumeration tools include OpUtils (*https://www.manageengine.com*) and Network Performance Monitor (*https://www.solarwinds.com*).



Working of SNMP

Community String:
CompInfo
IP: 10.10.2.1
MIB
Software version, hard drive space, session table
Community String: CompInfo
Community String: Alarm
IP: 10.10.2.15
Sends request for active session
(Community String: CompInfo, IP: 10.10.2.15)
Active Session Information (No. of sessions: 2, Comm: CompInfo, IP: 10.10.2.15)
Host X (SNMP Manager)
Host Y (SNMP Agent)
SNMPTRAP message for failed login
Community String: Alarm
IP: 10.10.2.12
Host Z (SNMP Manager)

If the community string does not match the string stored in the management information base (MIB) database, then host Y will send a community string to a pre-configured SNMP manager indicating the error

Working of SNMP

SNMP uses a disturbed architecture comprising SNMP managers, SNMP agents, and several related components. The following are some commands associated with SNMP.

- **GetRequest**: Used by the SNMP manager to request information from an SNMP agent
- **GetNextRequest**: Used by the SNMP manager continuously to retrieve all the data stored in an array or table
- **GetResponse**: Used by an SNMP agent to satisfy a request made by the SNMP manager
- **SetRequest**: Used by the SNMP manager to modify the value of a parameter within an SNMP agent's management information base (MIB)
- **Trap**: Used by an SNMP agent to inform the pre-configured SNMP manager of a certain event

The communication process between an SNMP manager and SNMP agent is as follows.

- The SNMP manager (Host X, 10.10.2.1) uses the GetRequest command to send a request for the number of active sessions to the SNMP agent (Host Y, 10.10.2.15). To perform this step, the SNMP manager uses an SNMP service library such as the Microsoft SNMP Management API library (Mgmtapi.dll) or Microsoft WinSNMP API library (Wsnmp32.dll).
- The SNMP agent (Host Y) receives the message and verifies if the community string (Compinfo) is present on its MIB, checks the request against its list of access permissions for that community, and verifies the source IP address.

- If the SNMP agent does not find the community string or access permission in Host Y's MIB database and the SNMP service is set to send an authentication trap, it sends an authentication failure trap to the specified trap destination, Host Z.
- The master agent component of the SNMP agent calls the appropriate extension agent to retrieve the requested session information from the MIB.
- Using the session information retrieved from the extension agent, the SNMP service forms a return SNMP message that contains the number of active sessions and the destination IP address (10.10.2.1) of the SNMP manager, Host X.
- Host Y sends the response to Host X.

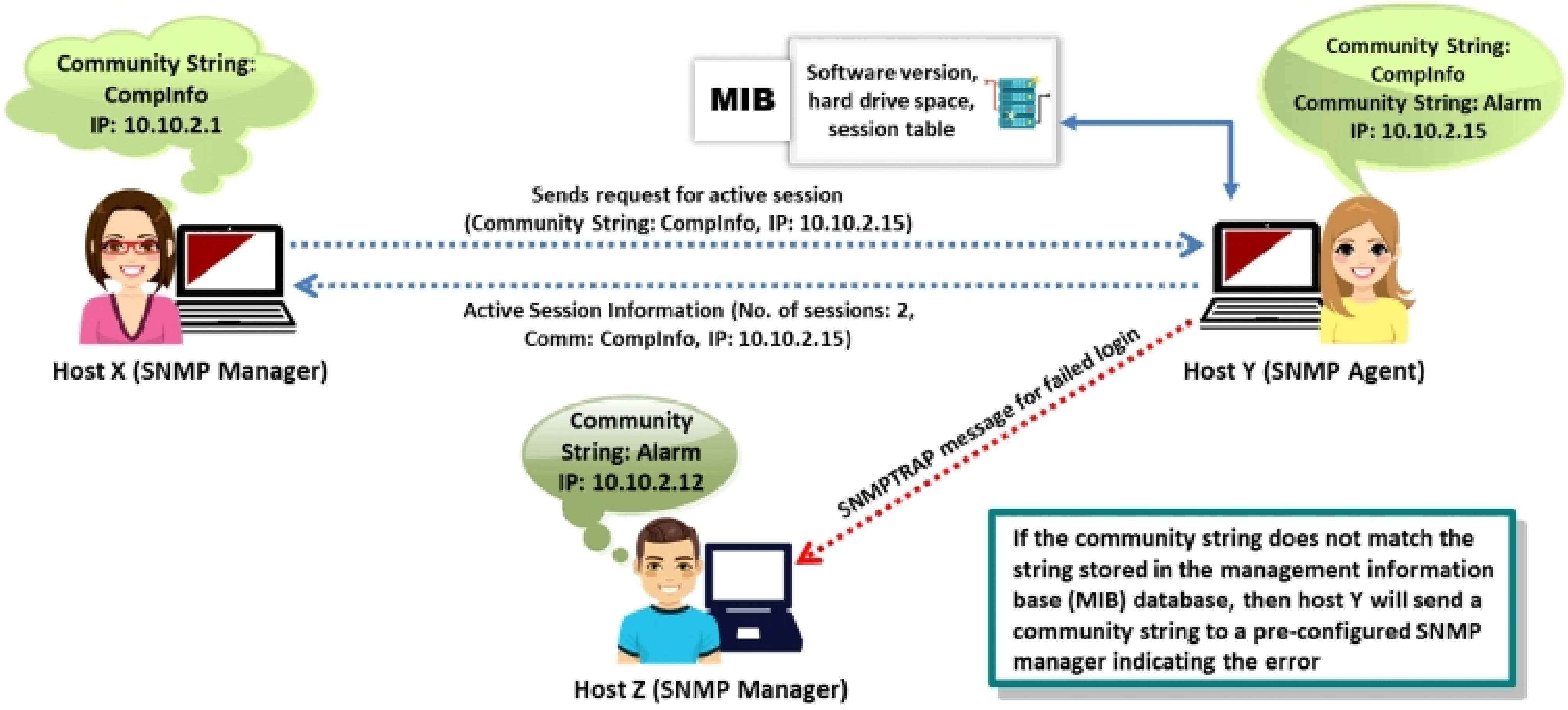
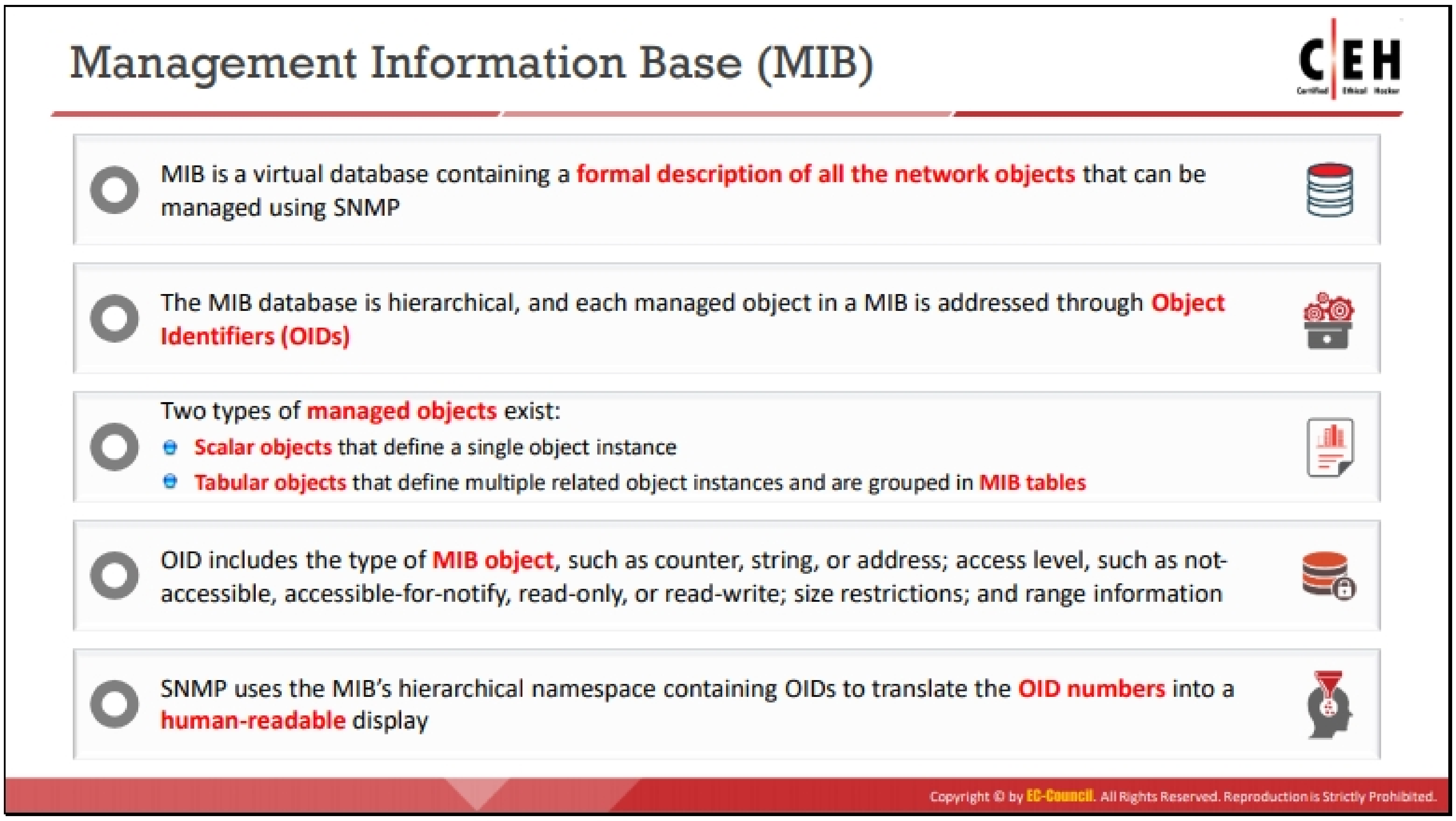

Community String: CompInfo IP: 10.10.2.1
MIB
Software version, hard drive space, session table
Community String: CompInfo Community String: Alarm IP: 10.10.2.15
Sends request for active session (Community String: CompInfo, IP: 10.10.2.15)
Active Session Information (No. of sessions: 2, Comm: CompInfo, IP: 10.10.2.15)
Host X (SNMP Manager)
Host Y (SNMP Agent)
SNMPTRAP message for failed login
Community String: Alarm IP: 10.10.2.12
Host Z (SNMP Manager)
If the community string does not match the string stored in the management information base (MIB) database, then host Y will send a community string to a pre-configured SNMP manager indicating the error

Figure 4.7: Illustration of the working of SNMP



Management Information Base (MIB)

- MIB is a virtual database containing a **formal description of all the network objects** that can be managed using SNMP
- The MIB database is hierarchical, and each managed object in a MIB is addressed through **Object Identifiers (OIDs)**
- Two types of **managed objects** exist:
  - **Scalar objects** that define a single object instance
  - **Tabular objects** that define multiple related object instances and are grouped in **MIB tables**
- OID includes the type of **MIB object**, such as counter, string, or address; access level, such as not-accessible, accessible-for-notify, read-only, or read-write; size restrictions; and range information
- SNMP uses the MIB's hierarchical namespace containing OIDs to translate the **OID numbers** into a **human-readable** display

Management Information Base (MIB)

MIB is a virtual database containing a formal description of all the network objects that SNMP manages. It is a collection of hierarchically organized information. It provides a standard representation of the SNMP agent's information and storage. MIB elements are recognized using object identifiers (OIDs). An OID is the numeric name given to an object and begins with the root of the MIB tree. The OID can uniquely identify the object in the MIB hierarchy.

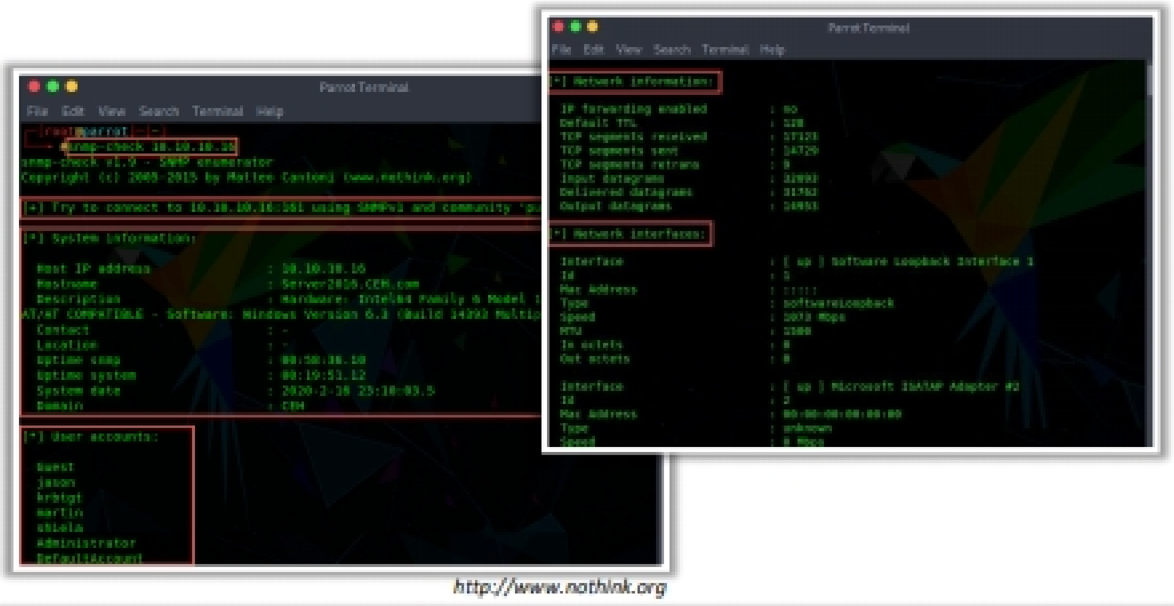
MIB-managed objects include scalar objects, which define a single object instance, and tabular objects, which define a group of related object instances. OIDs include the object's type (such as counter, string, or address), access level (such as read or read/write), size restrictions, and range information. The SNMP manager converts the OIDs into a human-readable display using the MIB as a codebook.

A user can access the contents of the MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. For example, http://IP.Address/Lseries.mib or http://library_name/Lseries.mib.Microsoft provides the list of MIBs that are installed with the SNMP service in the Windows resource kit. The major MIBs are .as follows:

- **DHCP.MIB**: Monitors network traffic between DHCP servers and remote hosts
- **HOSTMIB.MIB**: Monitors and manages host resources
- **LNMIB2.MIB**: Contains object types for workstation and server services
- **MIB_II.MIB:** Manages TCP/IP-based Internet using a simple architecture and system
- **WINS.MIB**: For the Windows Internet Name Service (WINS)

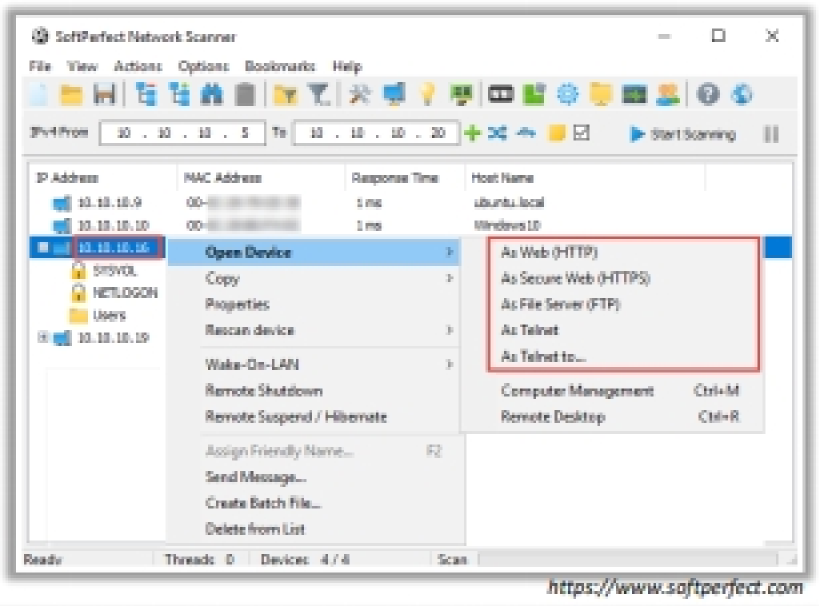
SNMP Enumeration Tools

Snmpcheck | Snmpcheck allows one to **enumerate** the **SNMP devices** and place the output in a very **human-readable** and friendly **format**



http://www.nothink.org

SoftPerfect Network Scanner | SoftPerfect Network Scanner **discovers shared folders** and retrieves practically any information about network devices **via WMI**, **SNMP**, **HTTP**, **SSH**, and **PowerShell**


SoftPerfect Network Scanner
File View Actions Options Bookmarks Help
IPv4 From 10 . 10 . 10 . 5 To 10 . 10 . 10 . 20
Start Scanning
IP Address
MAC Address
Response Time
Host Name
10.10.10.9
10.10.10.10
10.10.10.16
10.10.10.19
ubuntu.local
Windows10
SYSVOL
NETLOGON
Users
Open Device
Copy
Properties
Rescan device
Wake-On-LAN
Remote Shutdown
Remote Suspend / Hibernate
Assign Friendly Name...
Send Message...
Create Batch File...
Delete from List
As Web (HTTP)
As Secure Web (HTTPS)
As File Server (FTP)
As Telnet
As Telnet to...
Computer Management Ctrl+M
Remote Desktop Ctrl+R
Ready
Threads 0
Devices 4 / 4
Scan

https://www.softperfect.com

Other SNMP Enumeration Tools:

- **Network Performance Monitor** *https://www.solarwinds.com*
- **OpUtils** *https://www.manageengine.com*
- **PRTG Network Monitor** *https://www.paessler.com*
- **Engineer's Toolset** *https://www.solarwinds.com*

SNMP Enumeration Tools

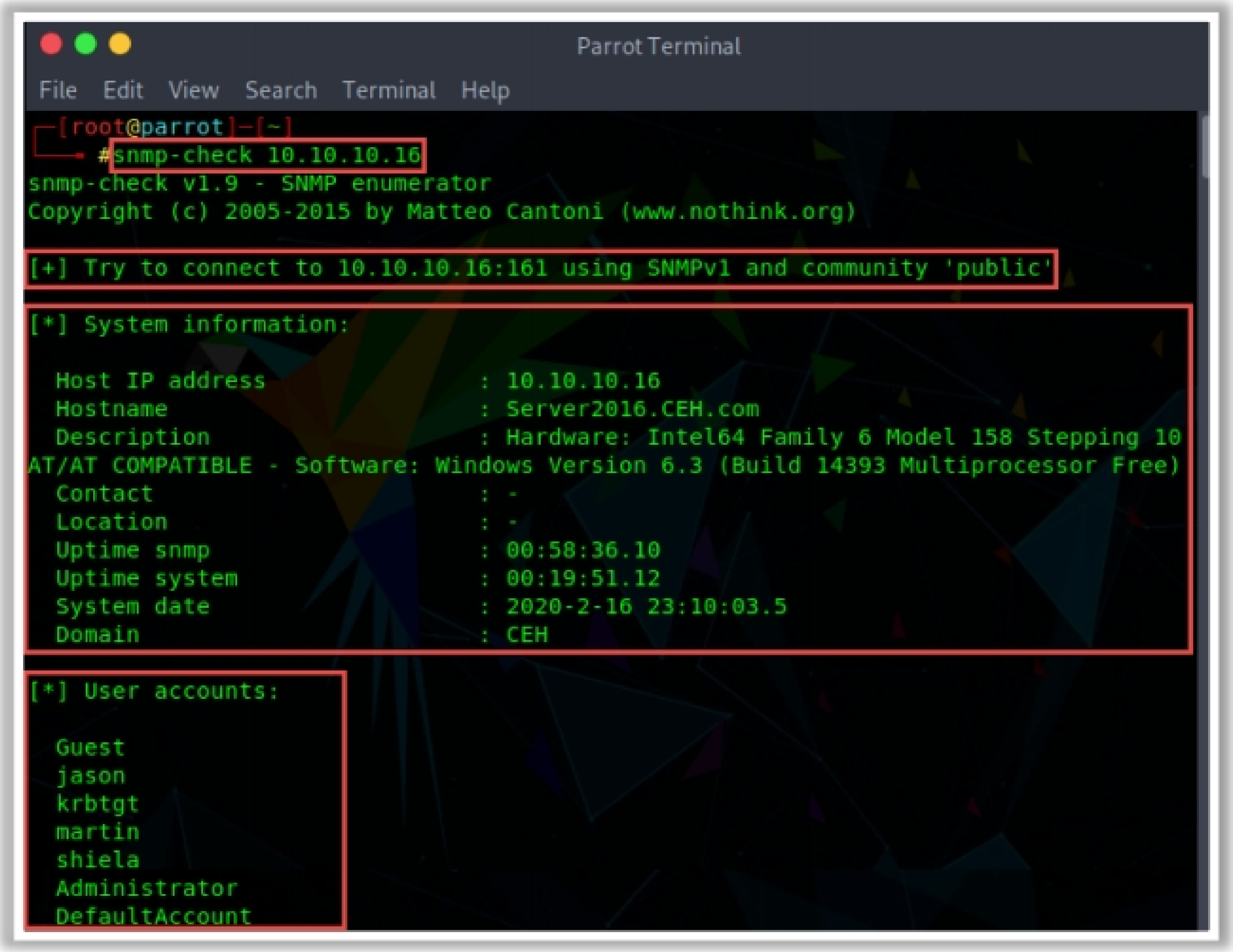
SNMP enumeration tools are used to scan a single IP address or a range of IP addresses of SNMP-enabled network devices to monitor, diagnose, and troubleshoot security threats.

- **Snmpcheck (snmp_enum Module)**

  Source: *http://www.nothink.org*

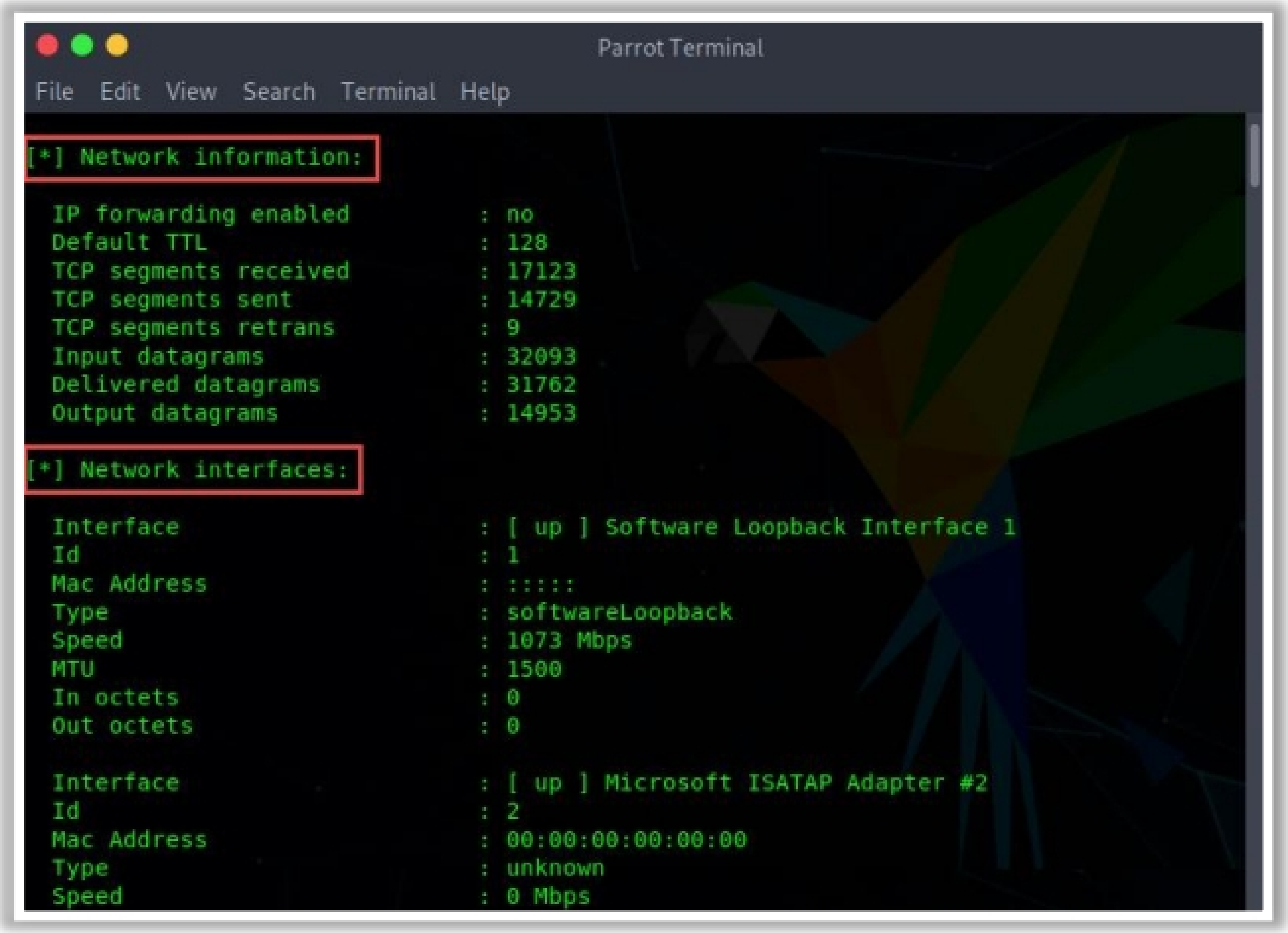
  Snmpcheck is an open-source tool distributed under the GNU General Public License (GPL). Its goal is to automate the process of gathering information on any device with SNMP support (Windows, Unix-like, network appliances, printers, etc.). Snmpcheck allows the enumeration of SNMP devices and places the output in a human-readable and user-friendly format. It could be useful for penetration testing or systems monitoring.

  Attackers use this tool to gather information about the target, such as contact, description, write access, devices, domain, hardware and storage information, hostname, Internet Information Services (IIS) statistics, IP forwarding, listening UDP ports, location, mountpoints, network interfaces, network services, routing information, software components, system uptime, TCP connections, total memory, uptime, and user accounts.



```
┌─[root@parrot]─[~]
└──╼ #snmp-check 10.10.10.16
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.10.10.16:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 10.10.10.16
  Hostname                      : Server2016.CEH.com
  Description                   : Hardware: Intel64 Family 6 Model 158 Stepping 10
AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 14393 Multiprocessor Free)
  Contact                       : -
  Location                      : -
  Uptime snmp                   : 00:58:36.10
  Uptime system                 : 00:19:51.12
  System date                   : 2020-2-16 23:10:03.5
  Domain                        : CEH

[*] User accounts:

  Guest
  jason
  krbtgt
  martin
  shiela
  Administrator
  DefaultAccount
```

Figure 4.8: Screenshot of snmpcheck showing system information and user accounts



```
[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 128
  TCP segments received         : 17123
  TCP segments sent             : 14729
  TCP segments retrans          : 9
  Input datagrams               : 32093
  Delivered datagrams           : 31762
  Output datagrams              : 14953

[*] Network interfaces:

  Interface                     : [ up ] Software Loopback Interface 1
  Id                            : 1
  Mac Address                   : :::::
  Type                          : softwareLoopback
  Speed                         : 1073 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ up ] Microsoft ISATAP Adapter #2
  Id                            : 2
  Mac Address                   : 00:00:00:00:00:00
  Type                          : unknown
  Speed                         : 0 Mbps
```

Figure 4.9: Screenshot of snmpcheck showing network information and interfaces

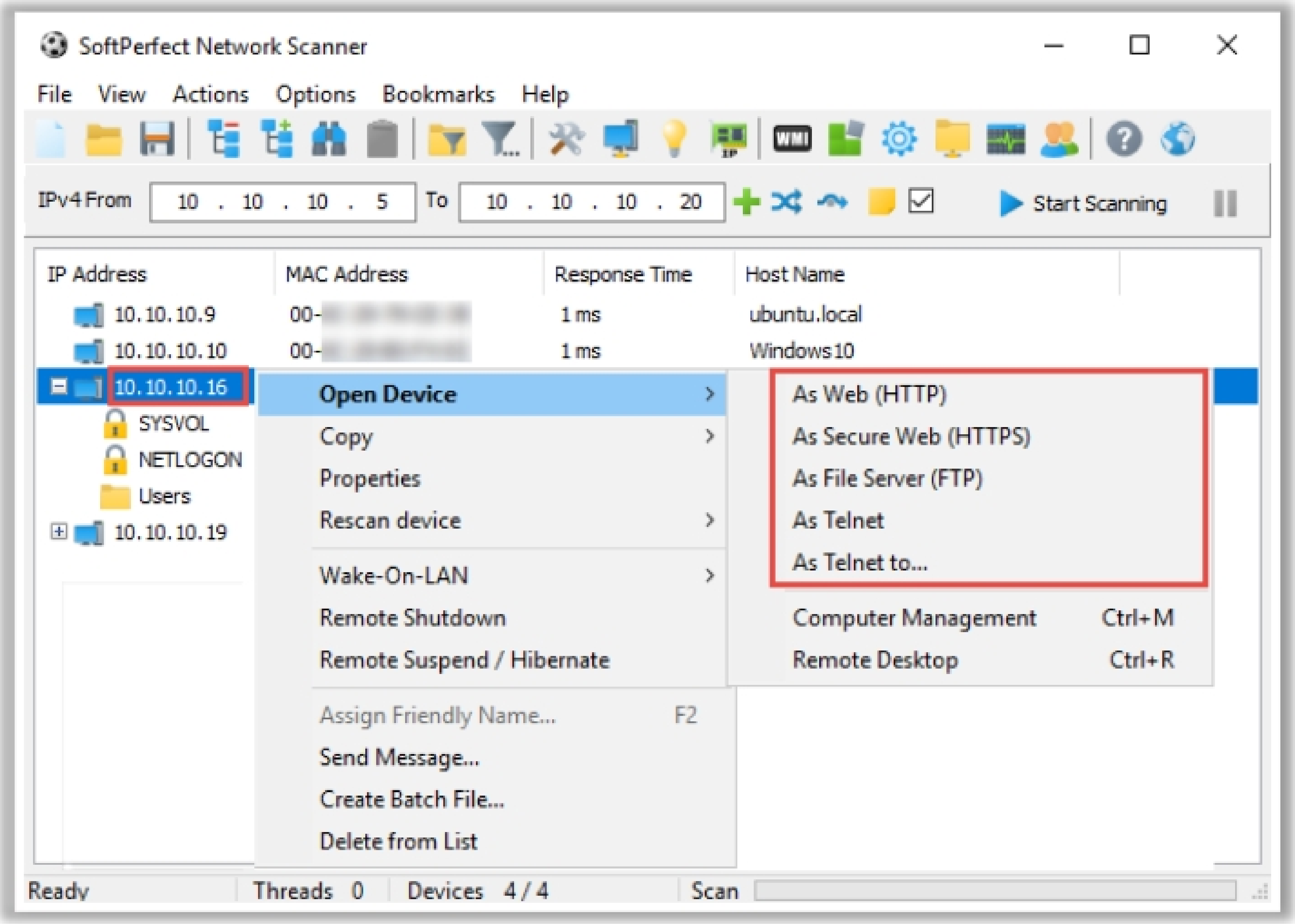
- **SoftPerfect Network Scanner**

  Source: *https://www.softperfect.com*

  SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices via Windows Management Instrumentation (WMI), SNMP, Hypertext Transfer Protocol (HTTP), SSH, and PowerShell. It also scans for remote services, registry, files, and performance counters; offers flexible filtering and display options; and exports NetScan results to a variety of formats ranging from Extensible Markup Language (XML) to JavaScript Object Notation (JSON).

  Moreover, SoftPerfect Network Scanner can check for a user-defined port and report if one is open. In addition, it can resolve host names and auto-detect the local and external IP range. It supports remote shutdown and Wake-on-LAN.

  Attackers uses this tool to gather information about a shared folder and network devices.


SoftPerfect Network Scanner
File
View
Actions
Options
Bookmarks
Help
Start Scanning
Open Device
Copy
Properties
Rescan device
Wake-On-LAN
Remote Shutdown
Remote Suspend / Hibernate
Assign Friendly Name... F2
Send Message...
Create Batch File...
Delete from List
As Web (HTTP)
As Secure Web (HTTPS)
As File Server (FTP)
As Telnet
As Telnet to...
Computer Management Ctrl+M
Remote Desktop Ctrl+R
Ready
Threads 0
Devices 4 / 4
Scan

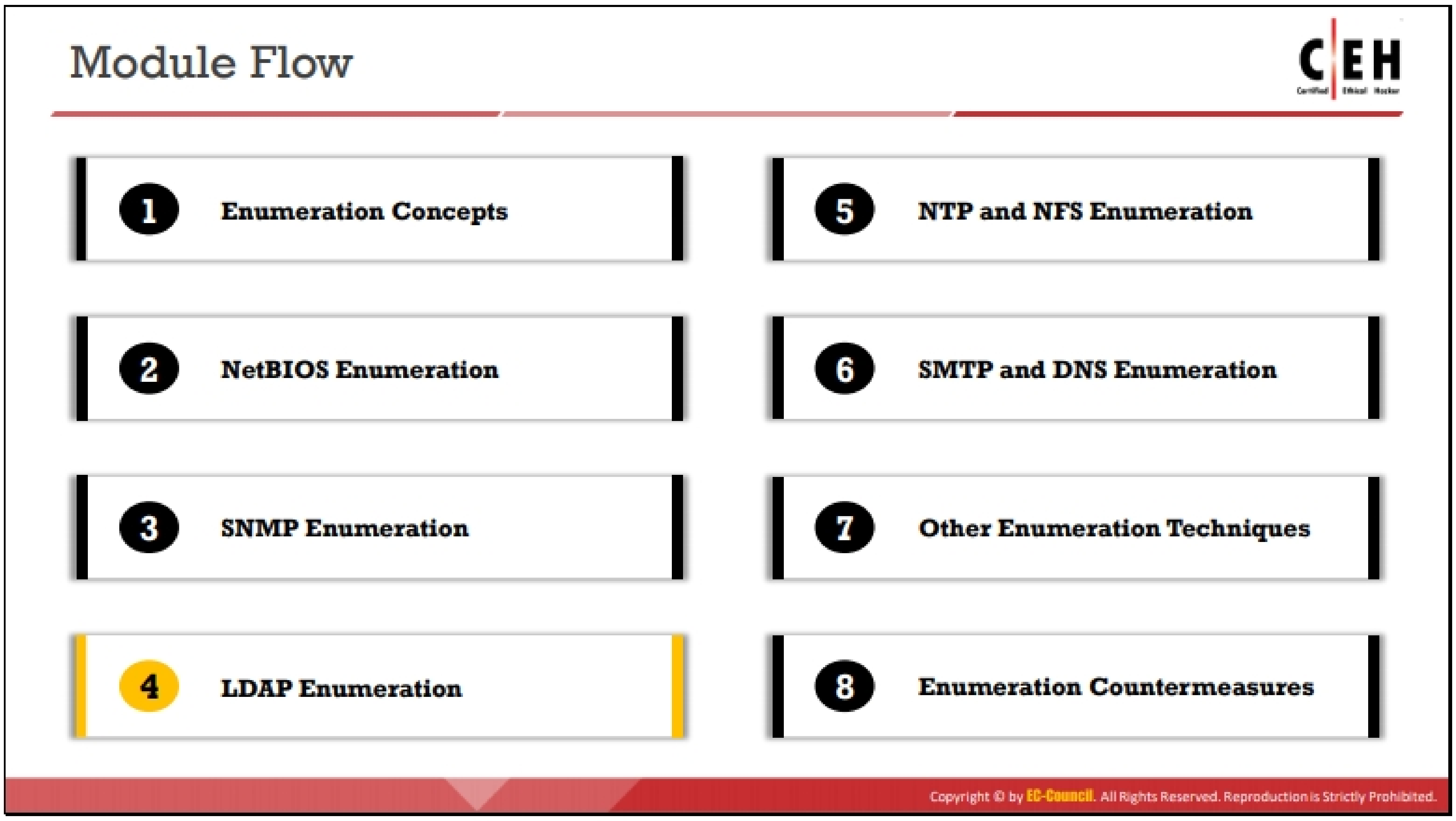
IPv4 From 10 . 10 . 10 . 5 To 10 . 10 . 10 . 20

IP Address	MAC Address	Response Time	Host Name
10.10.10.9	00-[redacted]	1 ms	ubuntu.local
10.10.10.10	00-[redacted]	1 ms	Windows10
10.10.10.16			
SYSVOL			
NETLOGON			
Users			
10.10.10.19			

Figure 4.10: Screenshot of SoftPerfect Network Scanner

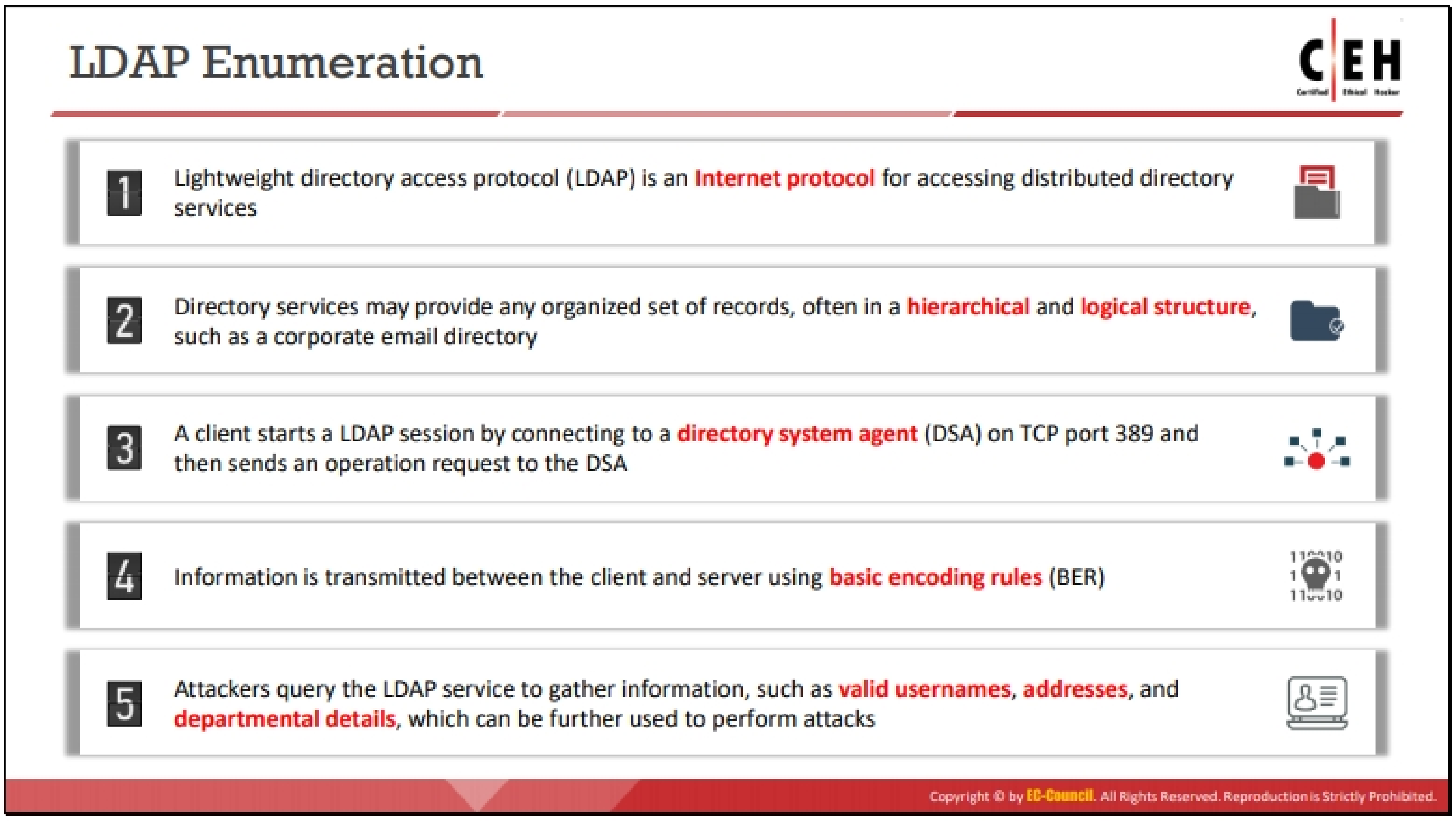
The following are some additional SNMP enumeration tools:

- Network Performance Monitor (*https://www.solarwinds.com*)
- OpUtils (*https://www.manageengine.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- Engineer's Toolset (*https://www.solarwinds.com*)



Module Flow

1. **Enumeration Concepts**
2. **NetBIOS Enumeration**
3. **SNMP Enumeration**
4. **LDAP Enumeration**
5. **NTP and NFS Enumeration**
6. **SMTP and DNS Enumeration**
7. **Other Enumeration Techniques**
8. **Enumeration Countermeasures**



LDAP Enumeration

1. Lightweight directory access protocol (LDAP) is an **Internet protocol** for accessing distributed directory services
2. Directory services may provide any organized set of records, often in a **hierarchical** and **logical structure**, such as a corporate email directory
3. A client starts a LDAP session by connecting to a **directory system agent** (DSA) on TCP port 389 and then sends an operation request to the DSA
4. Information is transmitted between the client and server using **basic encoding rules** (BER)
5. Attackers query the LDAP service to gather information, such as **valid usernames**, **addresses**, and **departmental details**, which can be further used to perform attacks

LDAP Enumeration

Various protocols enable communication and manage data transfer between network resources. All these protocols carry valuable information about network resources along with the data. An external user who successfully enumerates that information by manipulating the protocols can break into the network and may misuse the network resources. The Lightweight Directory Access Protocol (LDAP) is one such protocol that accesses the directory listings. This section focuses on

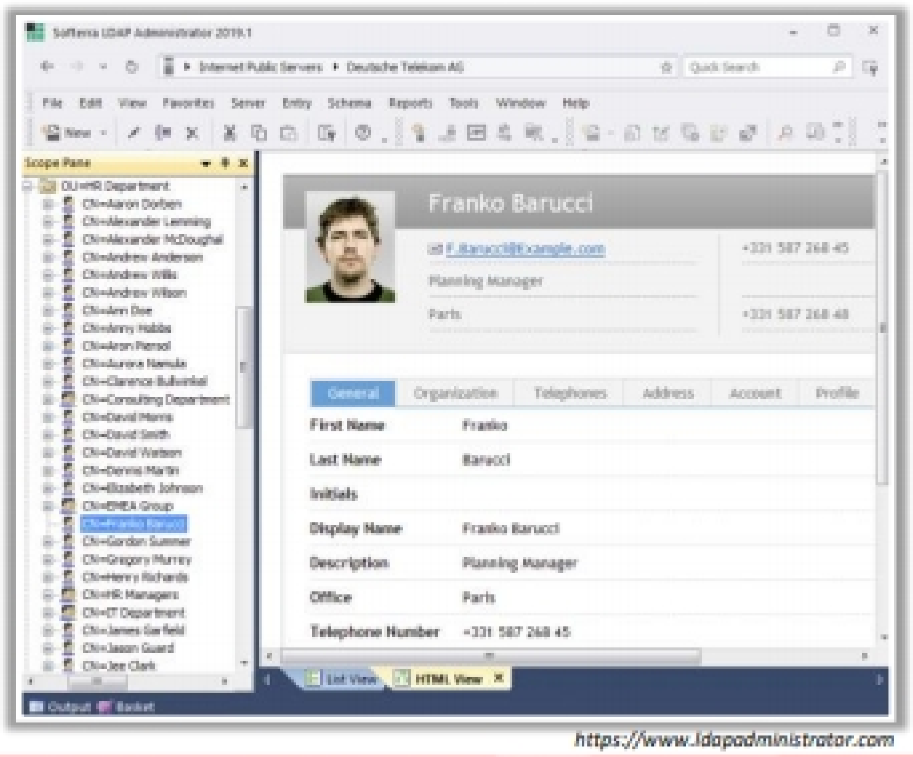
LDAP enumeration, the information extracted via LDAP enumeration, and LDAP enumeration tools.

LDAP is an Internet protocol for accessing distributed directory services. LDAP accesses directory listings within Active Directory or from other directory services. LDAP is a hierarchical or logical form of a directory, similar to a company's organizational chart. Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory. It uses DNS for quick lookups and the fast resolution of queries. A client starts an LDAP session by connecting to a Directory System Agent (DSA), typically on TCP port 389, and sends an operation request to the DSA. The Basic Encoding Rules (BER) format is used to transmit information between the client and server.

An attacker can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names, which an attacker can use to launch attacks.

LDAP Enumeration Tools

Softerra LDAP Administrator | Softerra LDAP Administrator provides various features essential for **LDAP development**, deployment, and **administration of directories**


Softerra LDAP Administrator 2019.1
Internet Public Servers ▸ Deutsche Telekom AG
Quick Search
File Edit View Favorites Server Entry Schema Reports Tools Window Help
New
Scope Pane
OU=HR Department
CN=Franko Barucci
General Organization Telephones Address Account Profile
List View
HTML View
Output
Basket

Franko Barucci

F.Barucci@Example.com

Planning Manager

Paris

+331 587 268 45

+331 587 268 48

First Name: Franko
Last Name: Barucci
Initials:
Display Name: Franko Barucci
Description: Planning Manager
Office: Paris
Telephone Number: +331 587 268 45

https://www.ldapadministrator.com

LDAP Admin Tool
https://www.ldapsoft.com

LDAP Account Manager
https://www.ldap-account-manager.org

LDAP Search
https://securityxploded.com

JXplorer
http://www.jxplorer.org

Active Directory Explorer (AD Explorer)
https://docs.microsoft.com

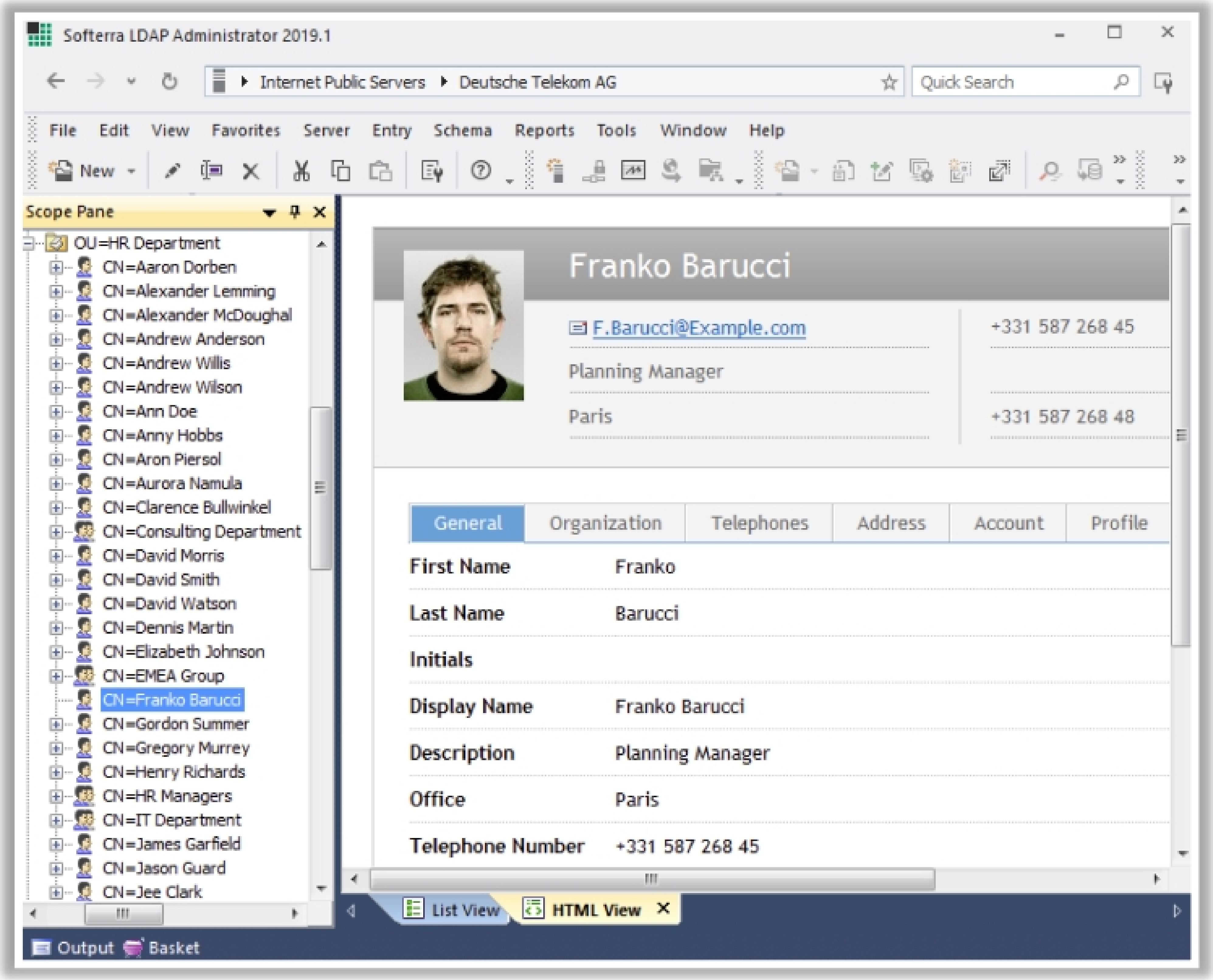
LDAP Enumeration Tools

There are many LDAP enumeration tools that access the directory listings within Active Directory or other directory services. By using these tools, attackers can enumerate information such as valid usernames, addresses, and departmental details from different LDAP servers.

- **Softerra LDAP Administrator**

  Source: *https://www.ldapadministrator.com*

  Softerra LDAP Administrator is an LDAP administration tool that works with LDAP servers such as Active Directory, Novell Directory Services, and Netscape/iPlanet. It browses and manages LDAP directories. As shown in the screenshot, attackers use Softerra LDAP Administrator to enumerate user details such as first name, last name, email address, designation, office location, and telephone number.

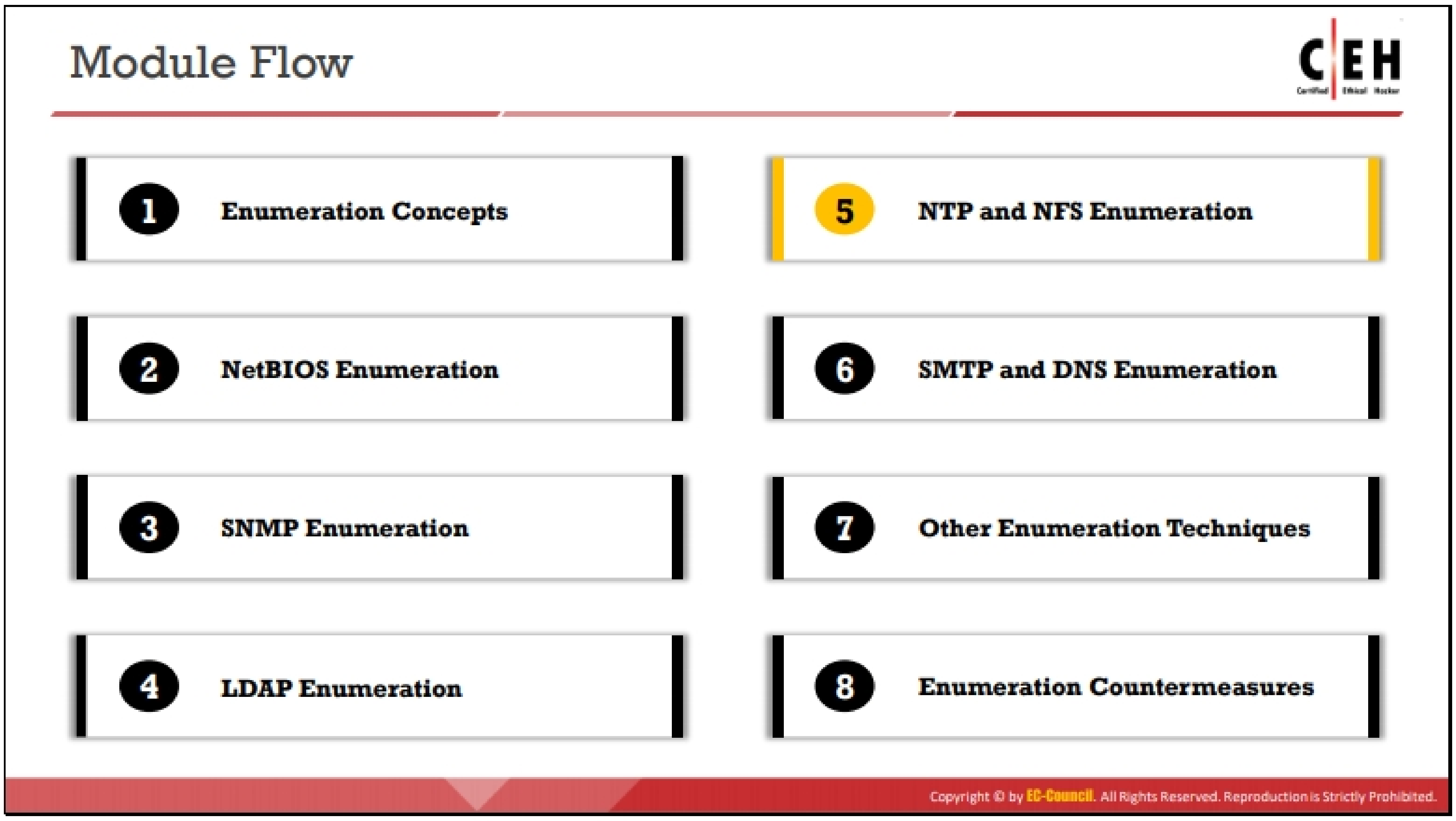

Softerra LDAP Administrator 2019.1
Internet Public Servers ▸ Deutsche Telekom AG
Quick Search
File Edit View Favorites Server Entry Schema Reports Tools Window Help
New
Scope Pane
OU=HR Department
CN=Aaron Dorben
CN=Alexander Lemming
CN=Alexander McDoughal
CN=Andrew Anderson
CN=Andrew Willis
CN=Andrew Wilson
CN=Ann Doe
CN=Anny Hobbs
CN=Aron Piersol
CN=Aurora Namula
CN=Clarence Bullwinkel
CN=Consulting Department
CN=David Morris
CN=David Smith
CN=David Watson
CN=Dennis Martin
CN=Elizabeth Johnson
CN=EMEA Group
CN=Franko Barucci
CN=Gordon Summer
CN=Gregory Murrey
CN=Henry Richards
CN=HR Managers
CN=IT Department
CN=James Garfield
CN=Jason Guard
CN=Jee Clark
Franko Barucci
F.Barucci@Example.com
Planning Manager
Paris
+331 587 268 45
+331 587 268 48
General
Organization
Telephones
Address
Account
Profile
List View
HTML View
Output
Basket

First Name	Franko
Last Name	Barucci
Initials	
Display Name	Franko Barucci
Description	Planning Manager
Office	Paris
Telephone Number	+331 587 268 45

Figure 4.11: Screenshot of Softerra LDAP Administrator

The following are some additional LDAP enumeration tools:

- LDAP Admin Tool (*https://www.ldapsoft.com*)
- LDAP Account Manager (*https://www.ldap-account-manager.org*)
- LDAP Search (*https://securityxploded.com*)
- JXplorer (*http://www.jxplorer.org*)
- Active Directory Explorer (AD Explorer) (*https://docs.microsoft.com*)



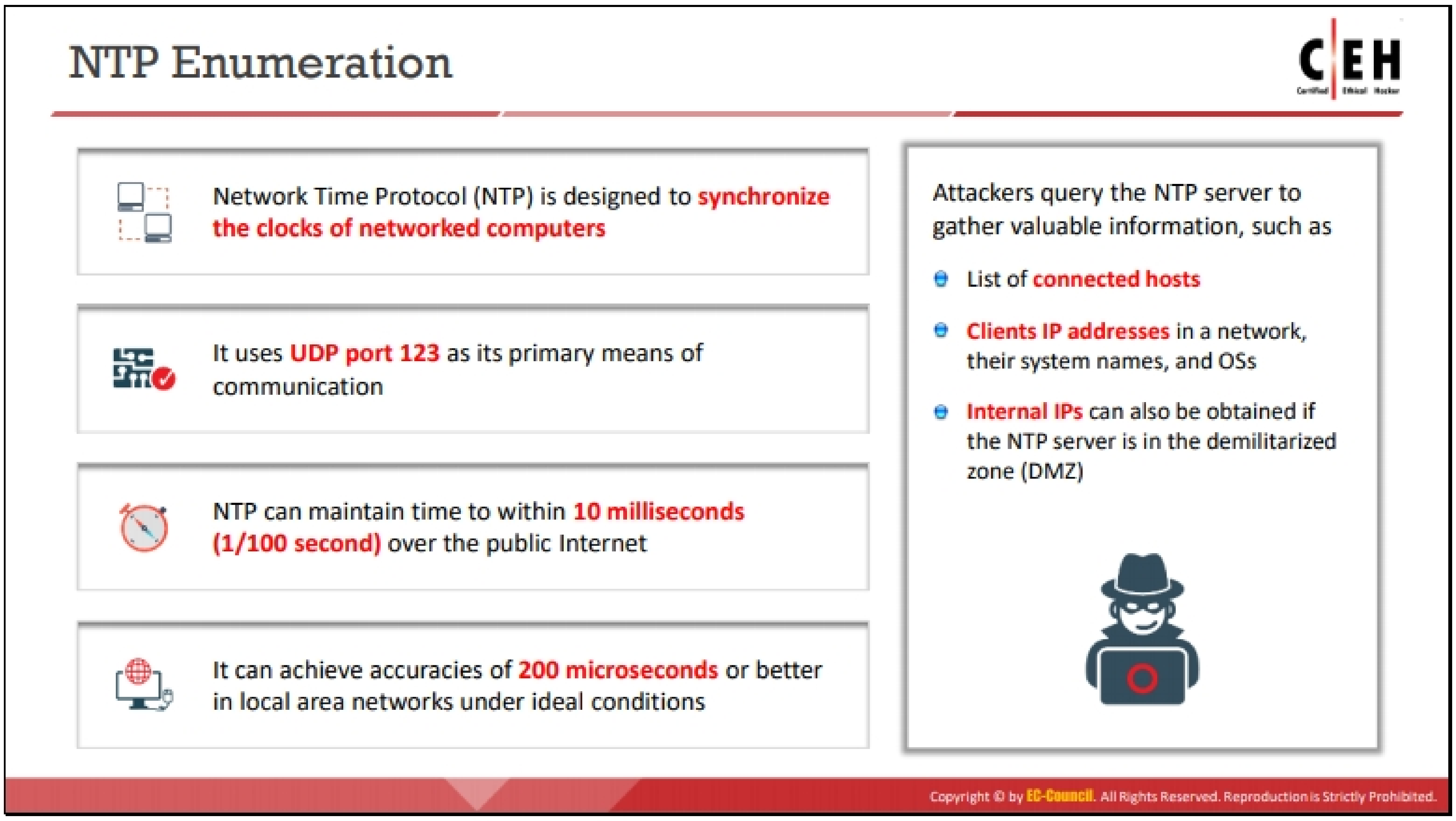
Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

NTP and NFS Enumeration

Administrators often overlook the Network Time Protocol (NTP) server when considering security. However, if queried properly, it can provide valuable network information to an attacker. Therefore, it is necessary to know what information an attacker can obtain about a network through NTP enumeration. The Network File System (NFS) is used for the management of remote file access. NFS enumeration helps attackers to gather information such as a list of clients connected to the NFS server, along with their IP addresses, and exported directories.

This section describes NTP enumeration, the information extracted via NTP enumeration, various NTP enumeration commands, NTP enumeration tools, and NFS enumeration techniques and tools.



NTP Enumeration

Network Time Protocol (NTP) is designed to **synchronize the clocks of networked computers**

It uses **UDP port 123** as its primary means of communication

NTP can maintain time to within **10 milliseconds (1/100 second)** over the public Internet

It can achieve accuracies of **200 microseconds** or better in local area networks under ideal conditions

Attackers query the NTP server to gather valuable information, such as

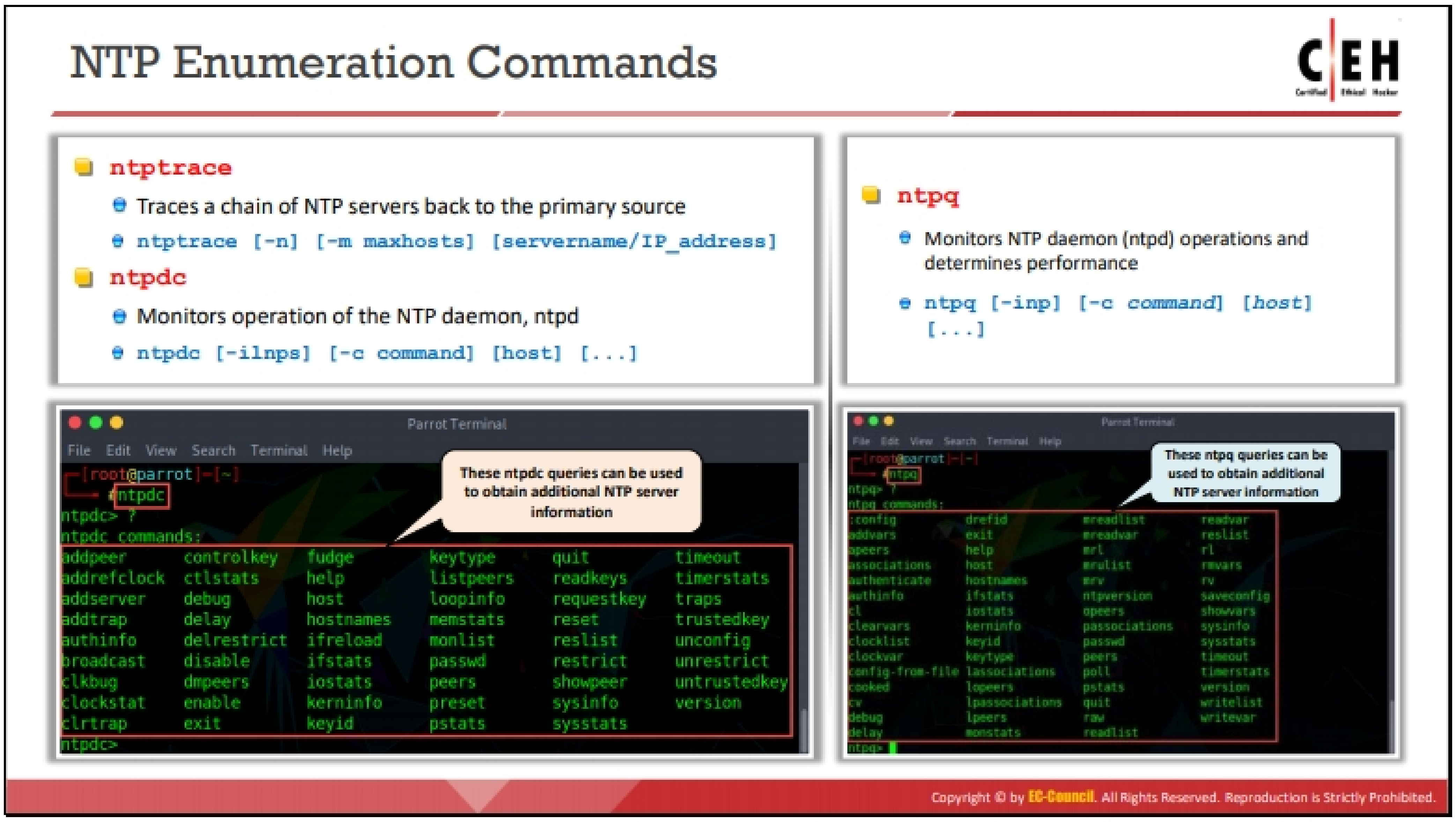
- List of **connected hosts**
- **Clients IP addresses** in a network, their system names, and OSs
- **Internal IPs** can also be obtained if the NTP server is in the demilitarized zone (DMZ)

NTP Enumeration

NTP is designed to synchronize clocks of networked computers. It uses UDP port 123 as its primary means of communication. NTP can maintain time within an error of 10 ms over the public Internet. Furthermore, it can achieve an accuracy of 200 µs or better in LANs under ideal conditions.

The following are some pieces of information an attacker can obtain by querying an NTP server:

- List of hosts connected to the NTP server
- Clients IP addresses in the network, their system names, and OSs
- Internal IPs, if the NTP server is in the demilitarized zone (DMZ)



NTP Enumeration Commands

- `ntptrace`
  - Traces a chain of NTP servers back to the primary source
  - `ntptrace [-n] [-m maxhosts] [servername/IP_address]`
- `ntpdc`
  - Monitors operation of the NTP daemon, ntpd
  - `ntpdc [-ilnps] [-c command] [host] [...]`
- `ntpq`
  - Monitors NTP daemon (ntpd) operations and determines performance
  - `ntpq [-inp] [-c command] [host] [...]`

```
┌─[root@parrot]─[~]
└──╼ #ntpdc
ntpdc> ?
ntpdc commands:
addpeer      controlkey   fudge        keytype      quit         timeout
addrefclock  ctlstats     help         listpeers    readkeys     timerstats
addserver    debug        host         loopinfo     requestkey   traps
addtrap      delay        hostnames    memstats     reset        trustedkey
authinfo     delrestrict  ifreload     monlist      reslist      unconfig
broadcast    disable      ifstats      passwd       restrict     unrestrict
clkbug       dmpeers      iostats      peers        showpeer     untrustedkey
clockstat    enable       kerninfo     preset       sysinfo      version
clrtrap      exit         keyid        pstats       sysstats
ntpdc>
```

These ntpdc queries can be used to obtain additional NTP server information

```
┌─[root@parrot]─[~]
└──╼ #ntpq
ntpq> ?
ntpq commands:
:config          drefid           mreadlist        readvar
addvars          exit             mreadvar         reslist
apeers           help             mrl              rl
associations     host             mrulist          rmvars
authenticate     hostnames        mrv              rv
authinfo         ifstats          ntpversion       saveconfig
cl               iostats          opeers           showvars
clearvars        kerninfo         passociations    sysinfo
clocklist        keyid            passwd           sysstats
clockvar         keytype          peers            timeout
config-from-file lassociations    poll             timerstats
cooked           lopeers          pstats           version
cv               lpassociations   quit             writelist
debug            lpeers           raw              writevar
delay            monstats         readlist
ntpq>
```

These ntpq queries can be used to obtain additional NTP server information

NTP Enumeration Commands

NTP enumeration commands such as **ntpdate, ntptrace, ntpdc,** and **ntpq** are used to query an NTP server for valuable information.

- **ntpdate**

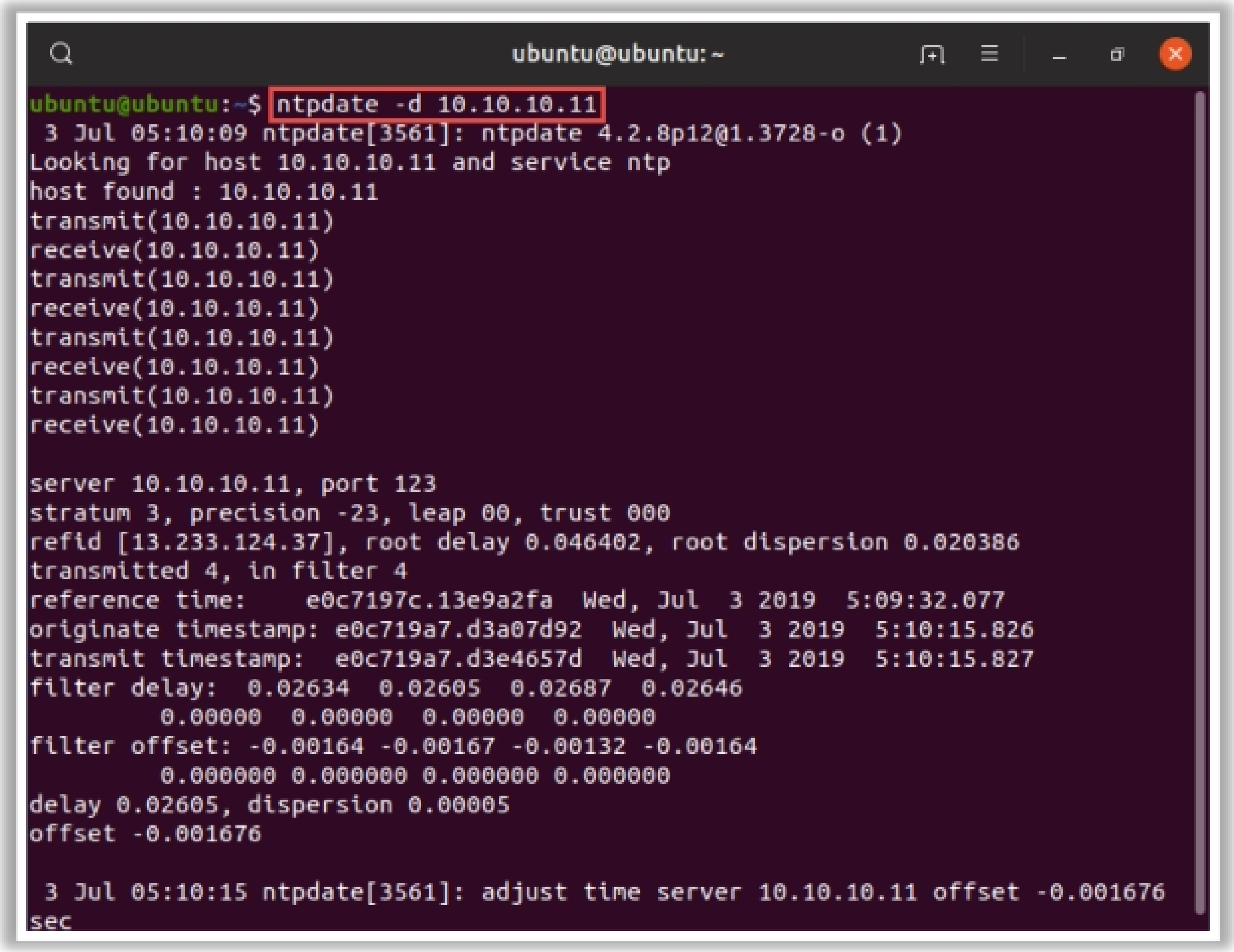
  This command collects the number of time samples from several time sources. Its syntax is as follows:

  ```
  ntpdate [-46bBdqsuv] [-a key] [-e authdelay] [-k keyfile] [-o version] [-p samples] [-t timeout] [ -U user_name] server [...]
  ```

-4	Force DNS resolution of given host names to the IPv4 namespace
-6	Force DNS resolution of given host names to the IPv6 namespace
-a key	Enable the authentication function/specify the key identifier to be used for authentication
-B	Force the time to always be slewed
-b	Force the time to be stepped
-d	Enable debugging mode
-e authdelay	Specify the processing delay to perform an authentication function
-k keyfile	Specify the path for the authentication key file as the string "keyfile"; the default is /etc/ntp/keys
-o version	Specify the NTP version for outgoing packets as an integer version, which can be 1 or 2; the default is 4

`-p samples`	Specify the number of samples to be acquired from each server, with values ranging from 1–8; the default is 4
`-q`	Query only; do not set the clock
`-s`	Divert logging output from the standard output (default) to the system syslog facility
`-t timeout`	Specify the maximum wait time for a server response; the default is 1 s
`-u`	Use an unprivileged port for outgoing packets
`-v`	Be verbose; logs ntpdate's version identification string

Table 4.4: ntpdate parameters and their respective functions



```
ubuntu@ubuntu:~$ ntpdate -d 10.10.10.11
 3 Jul 05:10:09 ntpdate[3561]: ntpdate 4.2.8p12@1.3728-o (1)
Looking for host 10.10.10.11 and service ntp
host found : 10.10.10.11
transmit(10.10.10.11)
receive(10.10.10.11)
transmit(10.10.10.11)
receive(10.10.10.11)
transmit(10.10.10.11)
receive(10.10.10.11)
transmit(10.10.10.11)
receive(10.10.10.11)

server 10.10.10.11, port 123
stratum 3, precision -23, leap 00, trust 000
refid [13.233.124.37], root delay 0.046402, root dispersion 0.020386
transmitted 4, in filter 4
reference time:    e0c7197c.13e9a2fa  Wed, Jul  3 2019  5:09:32.077
originate timestamp: e0c719a7.d3a07d92  Wed, Jul  3 2019  5:10:15.826
transmit timestamp:  e0c719a7.d3e4657d  Wed, Jul  3 2019  5:10:15.827
filter delay:  0.02634  0.02605  0.02687  0.02646
         0.00000  0.00000  0.00000  0.00000
filter offset: -0.00164 -0.00167 -0.00132 -0.00164
         0.000000 0.000000 0.000000 0.000000
delay 0.02605, dispersion 0.00005
offset -0.001676

 3 Jul 05:10:15 ntpdate[3561]: adjust time server 10.10.10.11 offset -0.001676
sec
```

Figure 4.12: Screenshot of the ntpdate command, showing debugging information for a given IP

- **ntptrace**

  This command determines where the NTP server obtains the time from and follows the chain of NTP servers back to its primary time source. Attackers use this command to trace the list of NTP servers connected to the network. Its syntax is as follows:

  `ntptrace [-n] [-m maxhosts] [servername/IP_address]`

`-n`	Do not print host names and show only IP addresses; may be useful if a name server is down
`-m maxhosts`	Set the maximum number of levels up the chain to be followed

Table 4.5: ntptrace parameters and their respective functions

Example:

```
# ntptrace
localhost: stratum 4, offset 0.0019529, synch distance 0.143235
10.10.0.1: stratum 2, offset 0.01142
73, synch distance 0.115554
10.10.1.1: stratum 1, offset 0.0017698, synch distance 0.011193
```

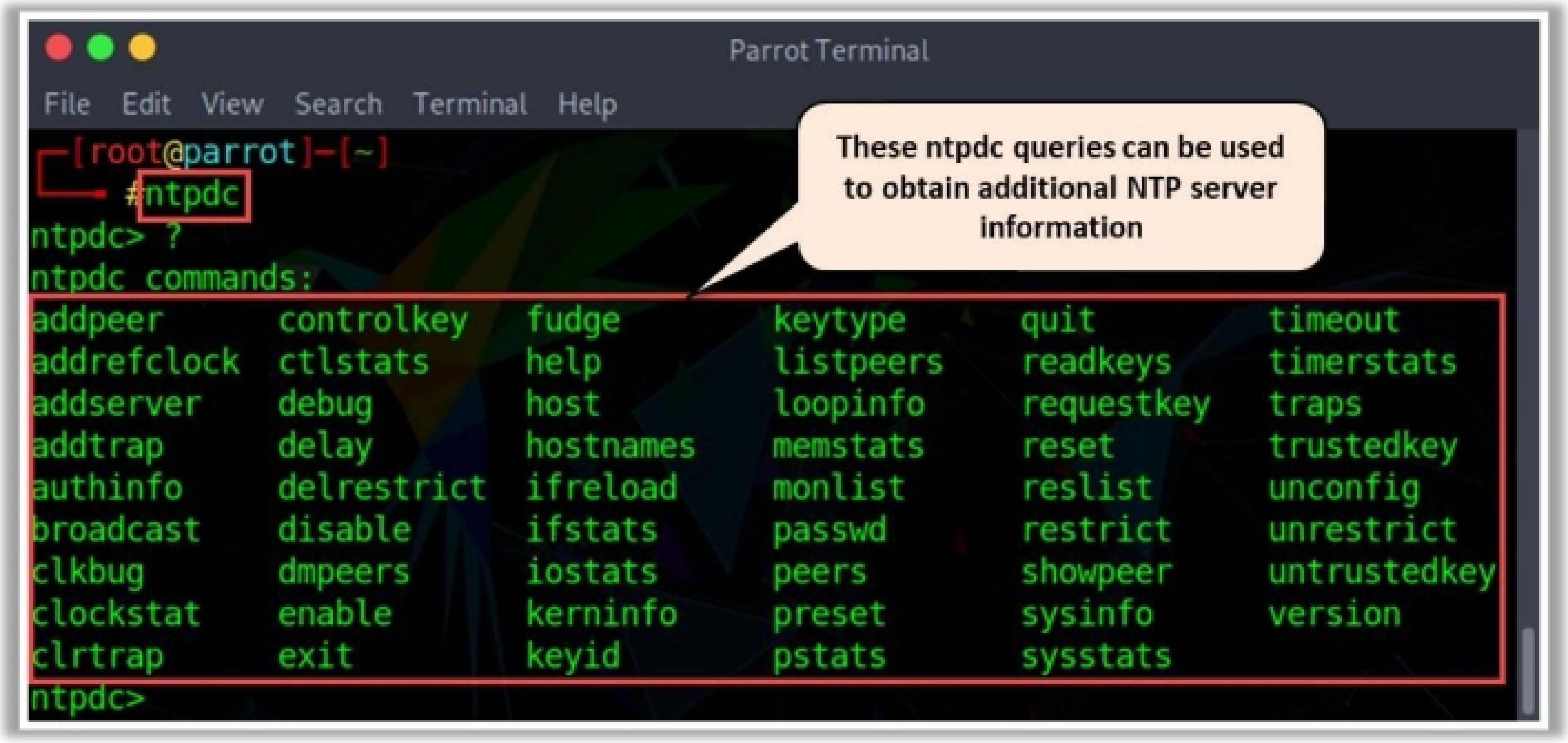
- **ntpdc**

  This command queries the ntpd daemon about its current state and requests changes in that state. Attackers use this command to retrieve the state and statistics of each NTP server connected to the target network. Its syntax is as follows:

  `ntpdc [-ilnps] [-c command] [hostname/IP_address]`

`-c`	Following argument interpreted as an interactive format command; multiple -c options may be given
`-i`	Force ntpdc to operate in the interactive mode
`-l`	Obtain a list of peers known to the server(s); this switch is equivalent to -c listpeers
`-n`	Output all host addresses in the dotted-quad numeric format, rather than host names
`-p`	Print a list of the peers as well as a summary of their states; this is equivalent to -c peers
`-s`	Print a list of the peers as well as a summary of their states, but in a slightly different format than the -p switch; this is equivalent to -c dmpeers.

Table 4.6: ntpdc parameters and their respective functions



```
┌─[root@parrot]─[~]
└──╼ #ntpdc
ntpdc> ?
ntpdc commands:
addpeer      controlkey   fudge        keytype      quit         timeout
addrefclock  ctlstats     help         listpeers    readkeys     timerstats
addserver    debug        host         loopinfo     requestkey   traps
addtrap      delay        hostnames    memstats     reset        trustedkey
authinfo     delrestrict  ifreload     monlist      reslist      unconfig
broadcast    disable      ifstats      passwd       restrict     unrestrict
clkbug       dmpeers      iostats      peers        showpeer     untrustedkey
clockstat    enable       kerninfo     preset       sysinfo      version
clrtrap      exit         keyid        pstats       sysstats
ntpdc>
```

These ntpdc queries can be used to obtain additional NTP server information

Figure 4.13: Screenshot of the ntpdc command

- **ntpq**

  This command monitors the operations of the NTP daemon **`ntpd`** and determines performance. Its syntax is as follows:

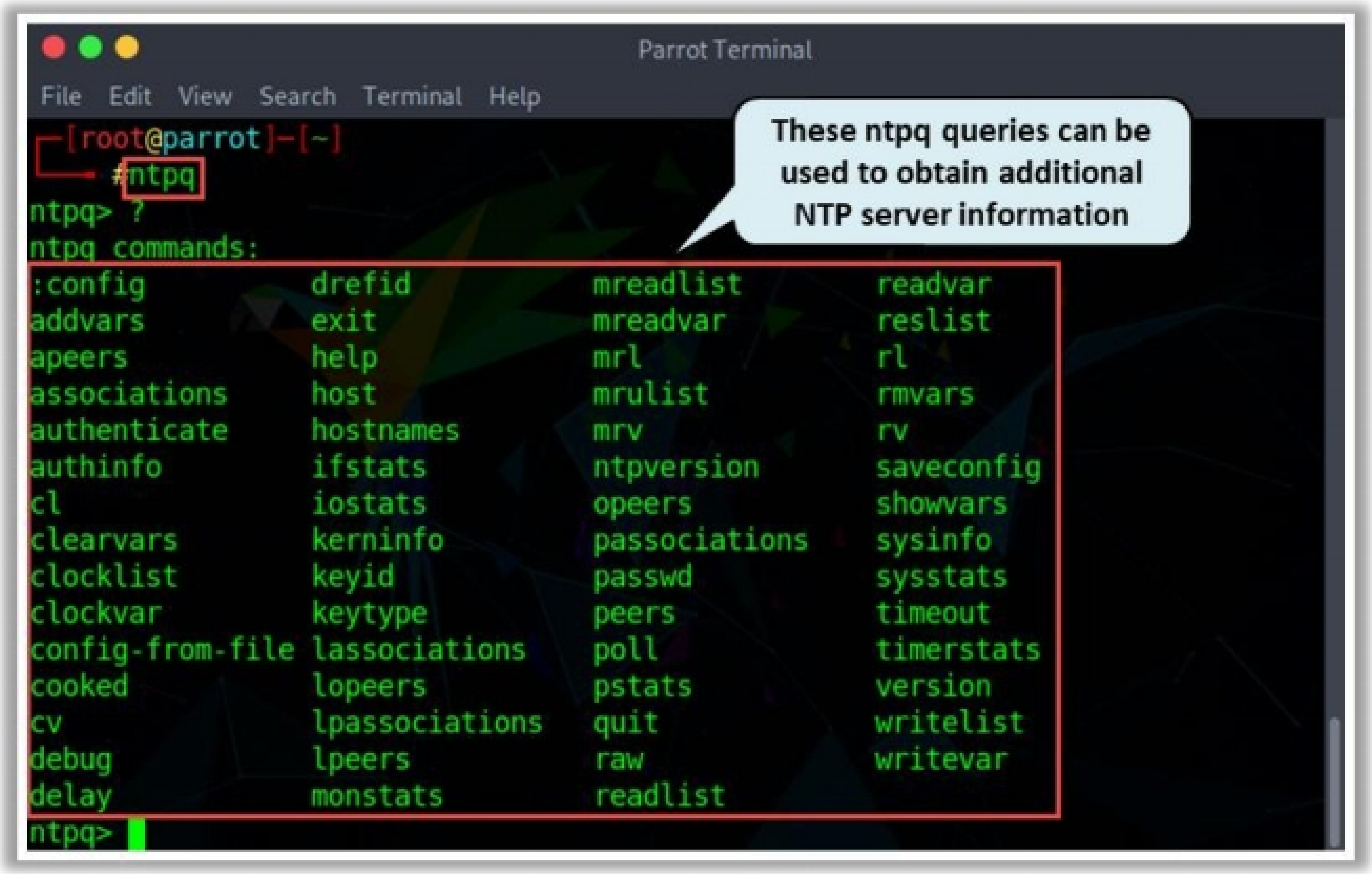
  `ntpq [-inp] [-c command] [host/IP_address]`

`-c`	Following argument is an interactive format command; multiple -c options may be given
`-d`	Debugging mode
`-i`	Force ntpq to operate in the interactive mode
`-n`	Output all host addresses in the dotted-quad numeric format, rather than host names
`-p`	Print a list of the peers as well as a summary of their states

Table 4.7: ntpq parameters and their respective functions

Example:

```
ntpq> version
ntpq 4.2.8p10@1.3728-o
ntpq> host
current host is localhost
```



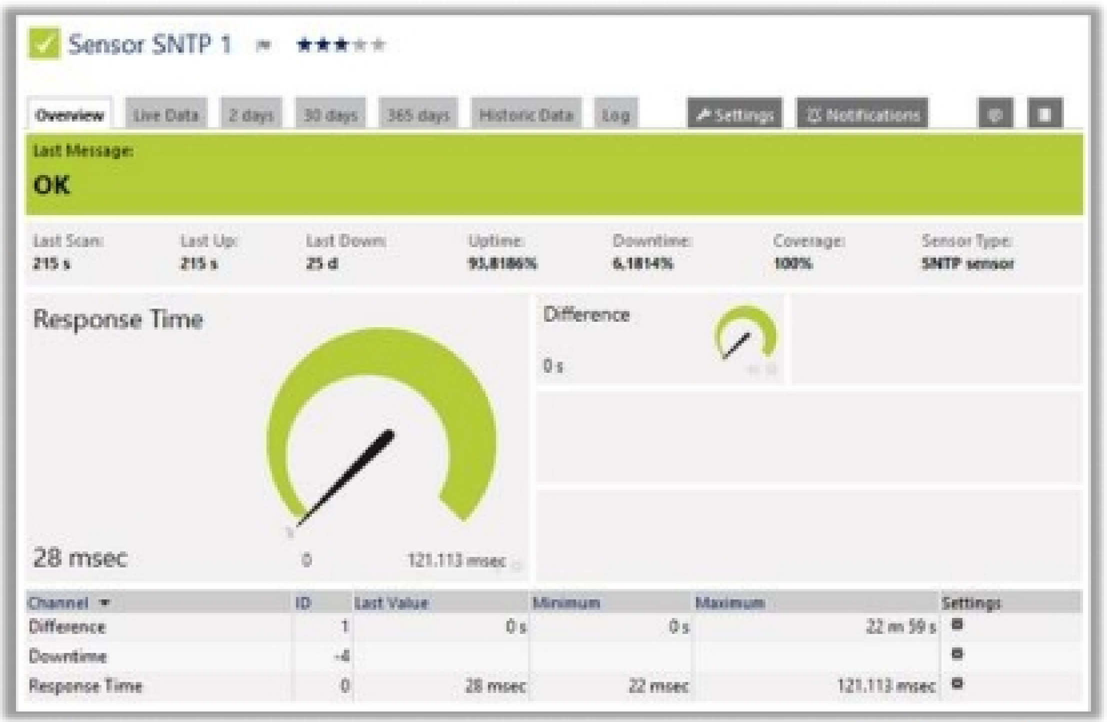
```
┌─[root@parrot]─[~]
└──╼ #ntpq
ntpq> ?
ntpq commands:
:config          drefid           mreadlist        readvar
addvars          exit             mreadvar         reslist
apeers           help             mrl              rl
associations     host             mrulist          rmvars
authenticate     hostnames        mrv              rv
authinfo         ifstats          ntpversion       saveconfig
cl               iostats          opeers           showvars
clearvars        kerninfo         passociations    sysinfo
clocklist        keyid            passwd           sysstats
clockvar         keytype          peers            timeout
config-from-file lassociations    poll             timerstats
cooked           lopeers          pstats           version
cv               lpassociations   quit             writelist
debug            lpeers           raw              writevar
delay            monstats         readlist
ntpq>
```

These ntpq queries can be used to obtain additional NTP server information

Figure 4.14: Screenshot of ntpq command

NTP Enumeration Tools

- **PRTG Network Monitor** includes **SNTP Sensor monitor**, a simple network time protocol (SNTP) server that shows the response time of the server and time difference in comparison to the local system time



Last Message:
OK

Last Scan:	Last Up:	Last Down:	Uptime:	Downtime:	Coverage:	Sensor Type:
215 s	215 s	25 d	93,8186%	6,1814%	100%	SNTP sensor

Channel ▼	ID	Last Value	Minimum	Maximum	Settings
Difference	1	0 s	0 s	22 m 59 s	■
Downtime	-4				■
Response Time	0	28 msec	22 msec	121.113 msec	■

https://www.paessler.com

NTP Enumeration Tools

- Nmap (*https://nmap.org*)
- Wireshark (*https://www.wireshark.org*)
- udp-proto-scanner (*https://labs.portcullis.co.uk*)
- NTP Server Scanner (*http://www.bytefusion.com*)

NTP Enumeration Tools

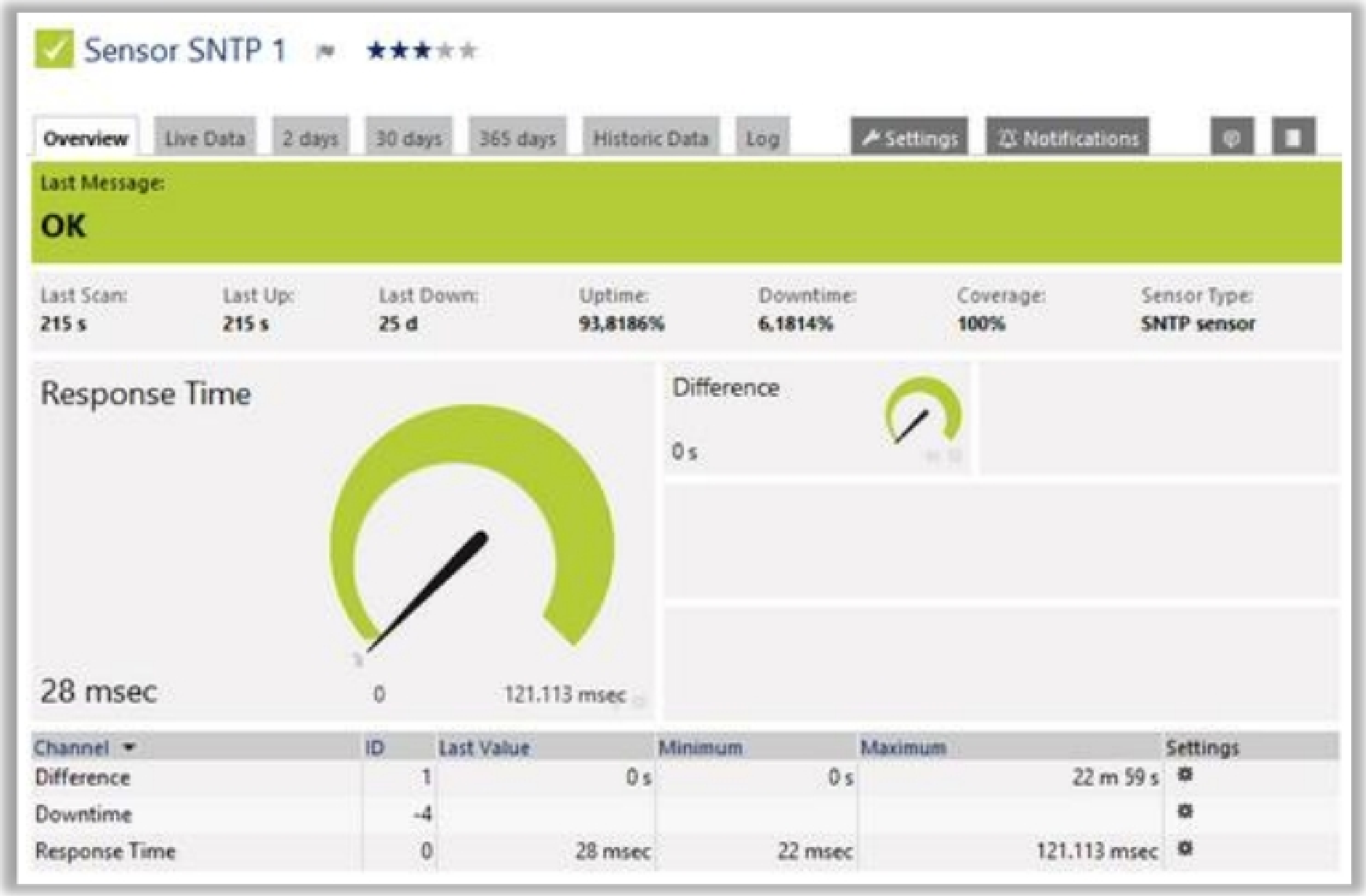
NTP enumeration tools are used to monitor the working of NTP and SNTP servers in the network and help in the configuration and verification of connectivity from the time client to the NTP servers.

- **PRTG Network Monitor**

  Source: *https://www.paessler.com*

  PRTG monitors all systems, devices, traffic, and applications of IT infrastructure by using various technologies such as SNMP, WMI, and SSH.

  As shown in the screenshot, attackers use PRTG Network Monitor to retrieve SNTP server details such as the response time from the server, active sensors with the server, and synchronization time.


Sensor SNTP 1
Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings
Notifications
Response Time
0
121.113 msec
Difference

Last Message:
OK

Last Scan:	Last Up:	Last Down:	Uptime:	Downtime:	Coverage:	Sensor Type:
215 s	**215 s**	**25 d**	**93,8186%**	**6,1814%**	**100%**	**SNTP sensor**

Response Time: 28 msec

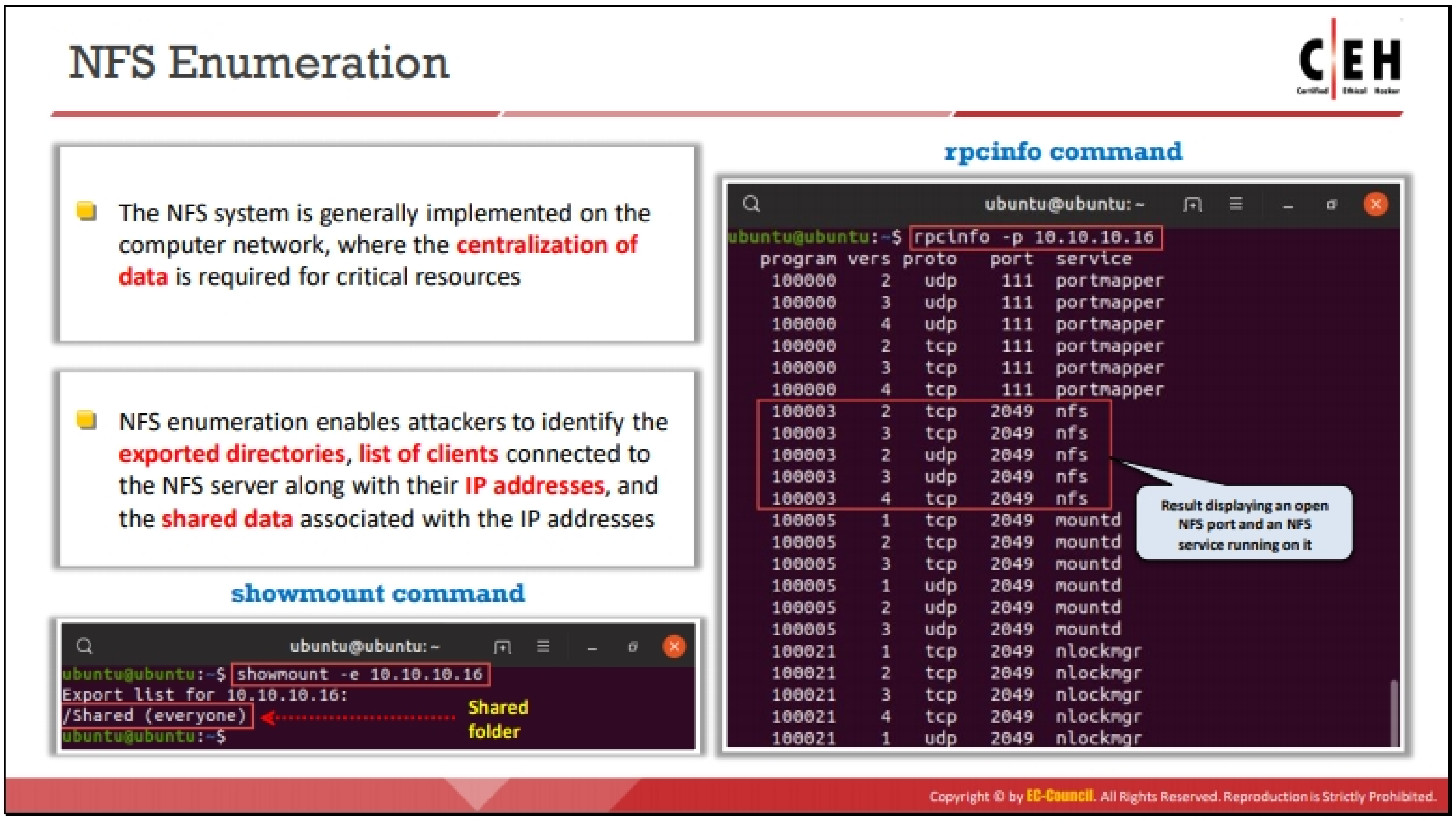
Difference: 0 s

Channel	ID	Last Value	Minimum	Maximum	Settings
Difference	1	0 s	0 s	22 m 59 s	⚙
Downtime	-4				⚙
Response Time	0	28 msec	22 msec	121.113 msec	⚙

Figure 4.15: Screenshot of PRTG Network Monitor

The following are some NTP enumeration tools:

- Nmap (*https://nmap.org*)
- Wireshark (*https://www.wireshark.org*)
- udp-proto-scanner (*https://labs.portcullis.co.uk*)
- NTP Server Scanner (*http://www.bytefusion.com*)



NFS Enumeration

- The NFS system is generally implemented on the computer network, where the **centralization of data** is required for critical resources
- NFS enumeration enables attackers to identify the **exported directories**, **list of clients** connected to the NFS server along with their **IP addresses**, and the **shared data** associated with the IP addresses

showmount command

```
ubuntu@ubuntu:~$ showmount -e 10.10.10.16
Export list for 10.10.10.16:
/Shared (everyone)
ubuntu@ubuntu:~$
```

rpcinfo command

```
ubuntu@ubuntu:~$ rpcinfo -p 10.10.10.16
   program vers proto   port  service
    100000    2   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    4   udp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    4   tcp    111  portmapper
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   tcp   2049  nfs
    100005    1   tcp   2049  mountd
    100005    2   tcp   2049  mountd
    100005    3   tcp   2049  mountd
    100005    1   udp   2049  mountd
    100005    2   udp   2049  mountd
    100005    3   udp   2049  mountd
    100021    1   tcp   2049  nlockmgr
    100021    2   tcp   2049  nlockmgr
    100021    3   tcp   2049  nlockmgr
    100021    4   tcp   2049  nlockmgr
    100021    1   udp   2049  nlockmgr
```

ubuntu@ubuntu: ~
Result displaying an open NFS port and an NFS service running on it

NFS Enumeration

NFS is a type of file system that enables users to access, view, store, and update files over a remote server. These remote data can be accessed by the client in the same way it is accessed on the local system. Depending on the privileges assigned to the clients, they can either only read or both read and write the data.

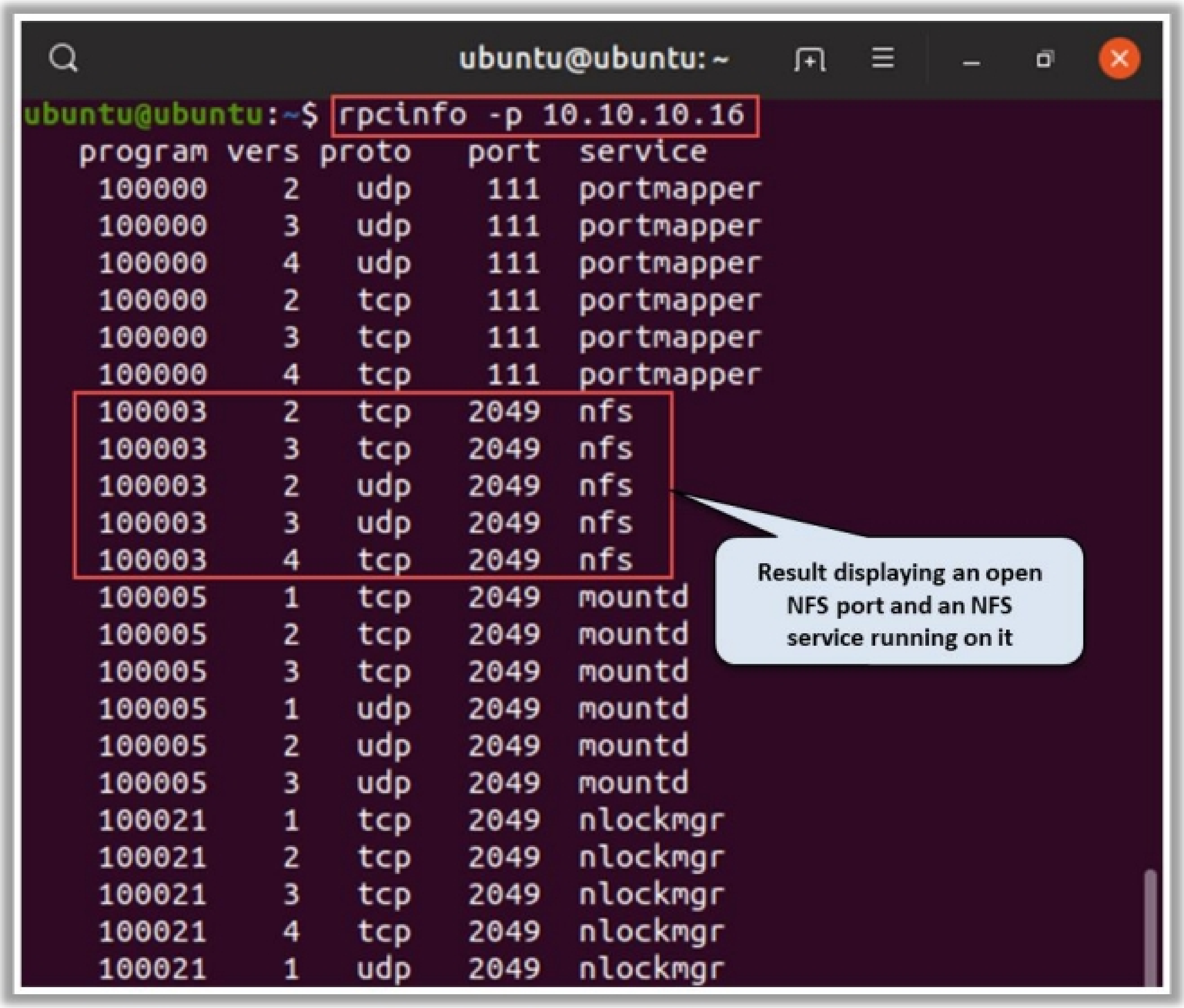
An NFS system is generally implemented on a computer network in which the centralization of data is required for critical resources. The remote procedure call (RPC) is used to route and process the request between clients and servers.

To accomplish the task of sharing files and directories over the network, the "exporting" process is used. However, the client first attempts to make the file available for sharing by using the "mounting" process. The `/etc/exports` location on the NFS server contains a list of clients allowed to share files on the server. In this approach, to access the server, the only credential used is the client's IP address. NFS versions before version 4 run on the same security specification.

Enumerating NFS services enables attackers to identify the exported directories, list of clients connected to the NFS server along with their IP addresses, and the shared data associated with the IP addresses. After gathering this information, the attackers can spoof their IP addresses to gain full access to the shared files on the server.

As shown in the screenshot, an attacker runs the following `rpcinfo` command to scan the target IP address for an open NFS port (port 2049) and the NFS services running on it:

```
rpcinfo -p 10.10.10.16
```



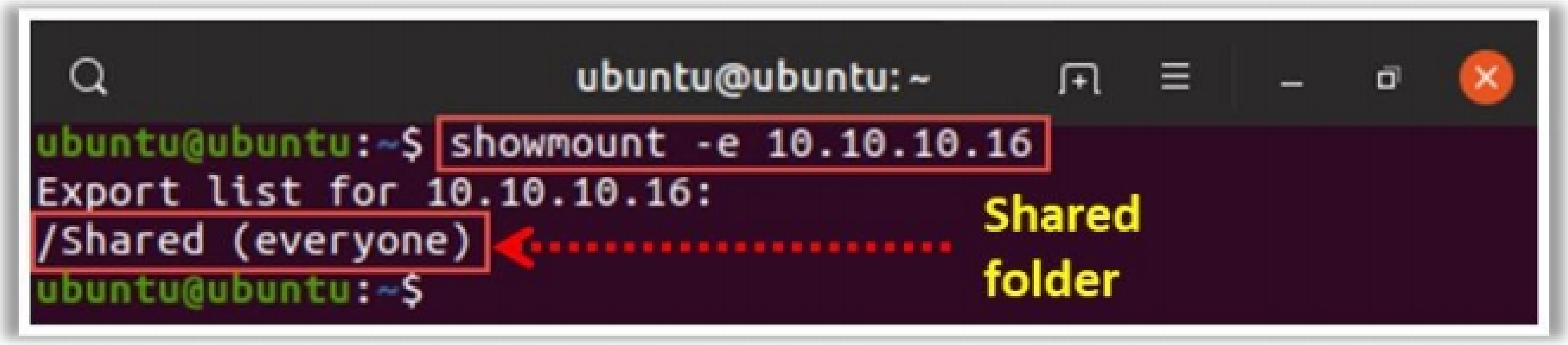
```
ubuntu@ubuntu:~$ rpcinfo -p 10.10.10.16
   program vers proto   port  service
    100000    2   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    4   udp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    4   tcp    111  portmapper
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   tcp   2049  nfs
    100005    1   tcp   2049  mountd
    100005    2   tcp   2049  mountd
    100005    3   tcp   2049  mountd
    100005    1   udp   2049  mountd
    100005    2   udp   2049  mountd
    100005    3   udp   2049  mountd
    100021    1   tcp   2049  nlockmgr
    100021    2   tcp   2049  nlockmgr
    100021    3   tcp   2049  nlockmgr
    100021    4   tcp   2049  nlockmgr
    100021    1   udp   2049  nlockmgr
```

Result displaying an open NFS port and an NFS service running on it

Figure 4.16: Screenshot of rpcinfo command displaying open NFS port and services

As shown in the screenshot, an attacker runs the following command to view the list of shared files and directories:

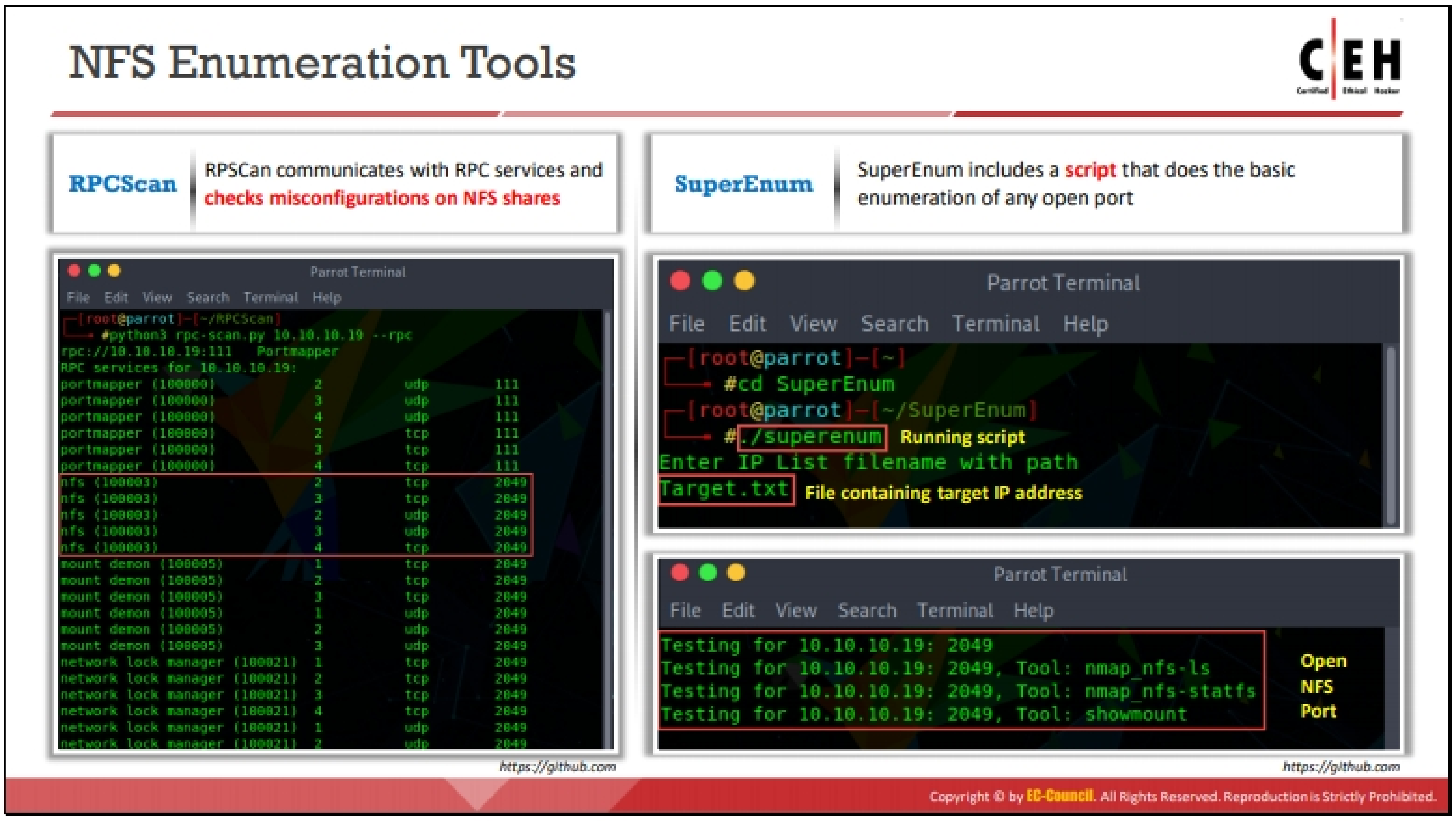
`showmount -e 10.10.10.16`



```
ubuntu@ubuntu:~$ showmount -e 10.10.10.16
Export list for 10.10.10.16:
/Shared (everyone)
ubuntu@ubuntu:~$
```

Figure 4.17: Screenshot of the showmount command displaying a shared directory

Further, an attacker can use various other commands and tools to gain access to the NFS server and upload malicious files on the server to launch further attacks.



NFS Enumeration Tools

RPCScan RPSCan communicates with RPC services and checks misconfigurations on NFS shares

```
┌─[root@parrot]─[~/RPCScan]
└──╼ #python3 rpc-scan.py 10.10.10.19 --rpc
rpc://10.10.10.19:111    Portmapper
RPC services for 10.10.10.19:
portmapper (100000)              2         udp        111
portmapper (100000)              3         udp        111
portmapper (100000)              4         udp        111
portmapper (100000)              2         tcp        111
portmapper (100000)              3         tcp        111
portmapper (100000)              4         tcp        111
nfs (100003)                     2         tcp        2049
nfs (100003)                     3         tcp        2049
nfs (100003)                     2         udp        2049
nfs (100003)                     3         udp        2049
nfs (100003)                     4         tcp        2049
mount demon (100005)             1         tcp        2049
mount demon (100005)             2         tcp        2049
mount demon (100005)             3         tcp        2049
mount demon (100005)             1         udp        2049
mount demon (100005)             2         udp        2049
mount demon (100005)             3         udp        2049
network lock manager (100021)    1         tcp        2049
network lock manager (100021)    2         tcp        2049
network lock manager (100021)    3         tcp        2049
network lock manager (100021)    4         tcp        2049
network lock manager (100021)    1         udp        2049
network lock manager (100021)    2         udp        2049
```

https://github.com

SuperEnum SuperEnum includes a script that does the basic enumeration of any open port

```
┌─[root@parrot]─[~]
└──╼ #cd SuperEnum
┌─[root@parrot]─[~/SuperEnum]
└──╼ #./superenum
Enter IP List filename with path
Target.txt
```

Running script

File containing target IP address

```
Testing for 10.10.10.19: 2049
Testing for 10.10.10.19: 2049, Tool: nmap_nfs-ls
Testing for 10.10.10.19: 2049, Tool: nmap_nfs-statfs
Testing for 10.10.10.19: 2049, Tool: showmount
```

Open NFS Port

https://github.com

NFS Enumeration Tools

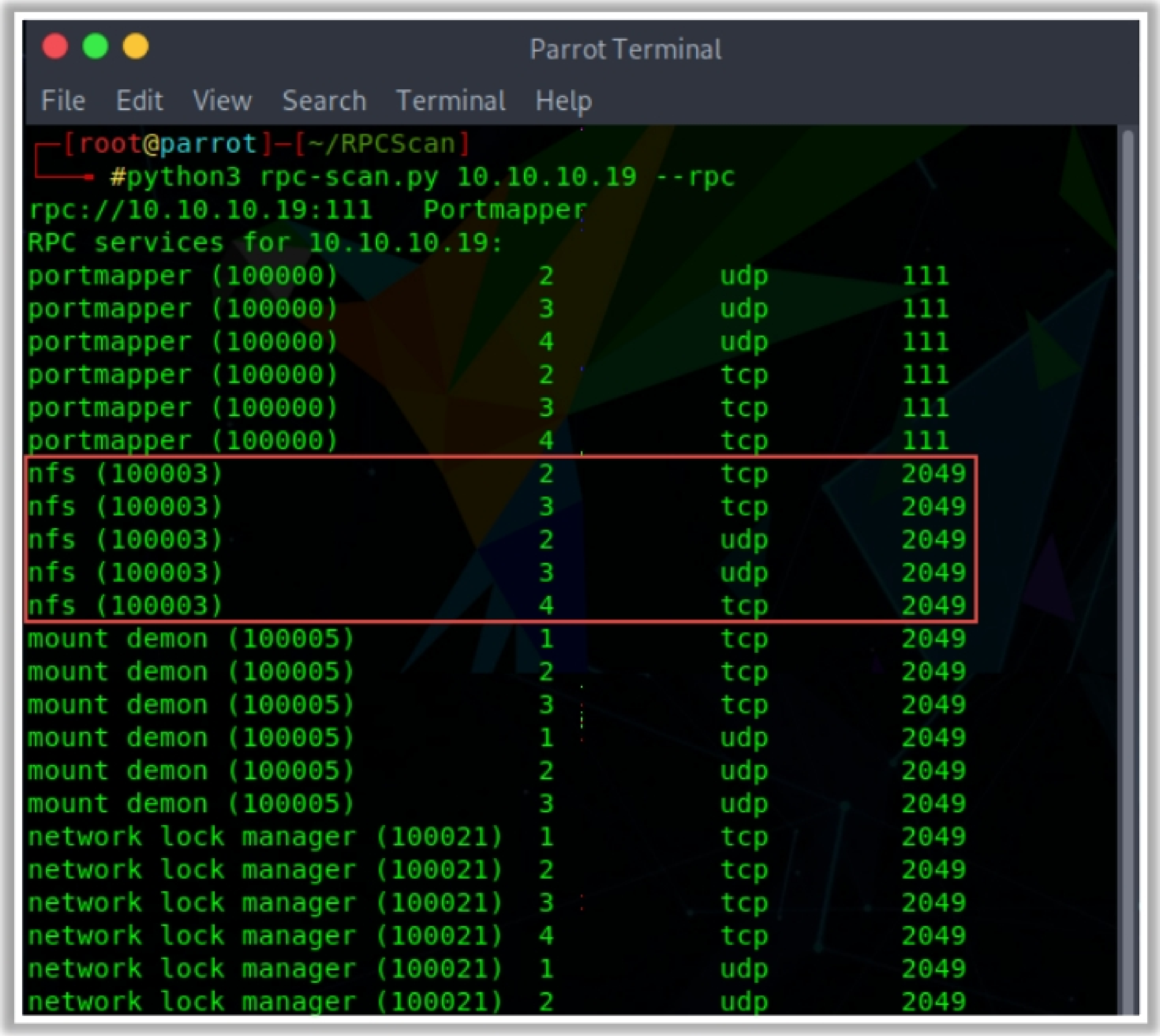
NFS enumeration tools scan a network within a given range of IP addresses or a single IP address to identify the NFS services running on it. These tools also assist in obtaining a list of RPC services using portmap, a list of NFS shares, and a list of directories accessible through NFS; further, they allow downloading a file shared through the NFS server. Attackers use tools such as RPCScan and SuperEnum to perform NFS enumeration.

- **RPCScan**

  Source: *https://github.com*

  RPCScan communicates with RPC services and checks misconfigurations on NFS shares. As shown in the screenshot, an attacker runs the following command to enumerate a target IP address for active NFS services:

  ```
  Python3 rpc-scan.py 10.10.10.19 --rpc
  ```



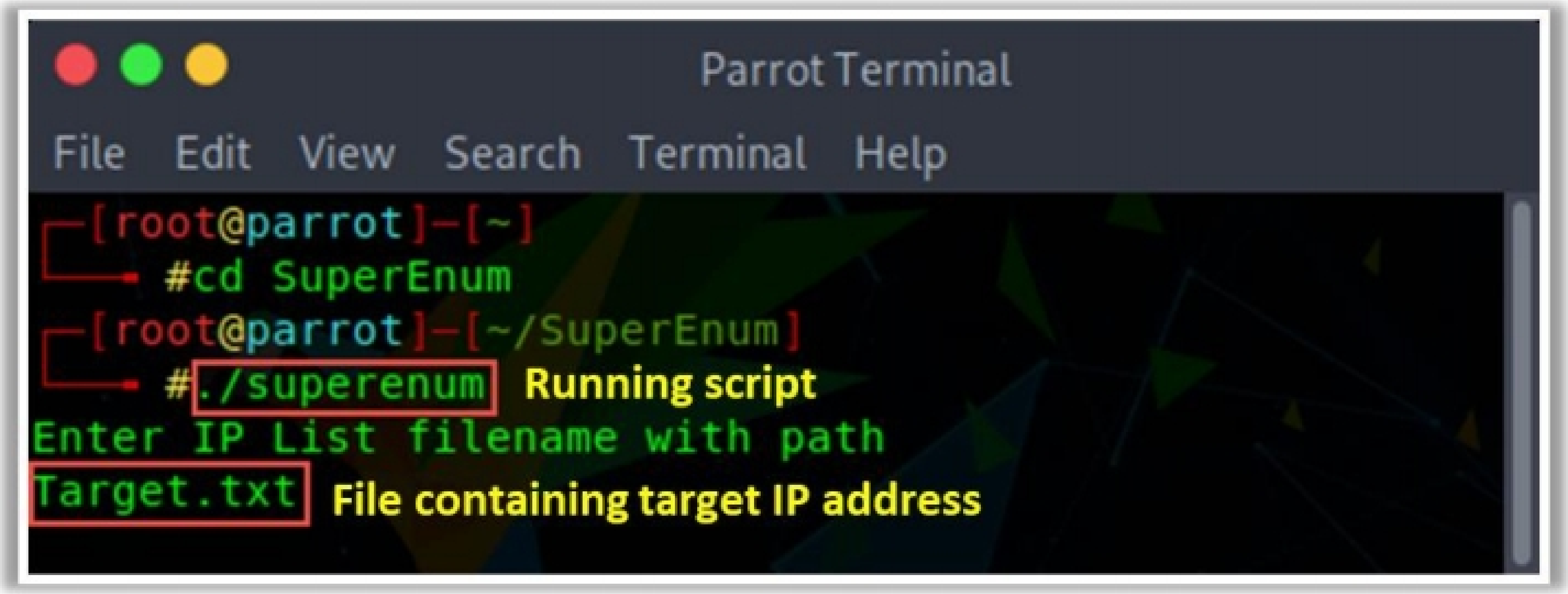
```
┌─[root@parrot]─[~/RPCScan]
└──╼ #python3 rpc-scan.py 10.10.10.19 --rpc
rpc://10.10.10.19:111   Portmapper
RPC services for 10.10.10.19:
portmapper (100000)             2           udp          111
portmapper (100000)             3           udp          111
portmapper (100000)             4           udp          111
portmapper (100000)             2           tcp          111
portmapper (100000)             3           tcp          111
portmapper (100000)             4           tcp          111
nfs (100003)                    2           tcp          2049
nfs (100003)                    3           tcp          2049
nfs (100003)                    2           udp          2049
nfs (100003)                    3           udp          2049
nfs (100003)                    4           tcp          2049
mount demon (100005)            1           tcp          2049
mount demon (100005)            2           tcp          2049
mount demon (100005)            3           tcp          2049
mount demon (100005)            1           udp          2049
mount demon (100005)            2           udp          2049
mount demon (100005)            3           udp          2049
network lock manager (100021)   1           tcp          2049
network lock manager (100021)   2           tcp          2049
network lock manager (100021)   3           tcp          2049
network lock manager (100021)   4           tcp          2049
network lock manager (100021)   1           udp          2049
network lock manager (100021)   2           udp          2049
```

Figure 4.18: Screenshot of RPCScan displaying open NFS ports and services

- **SuperEnum**

  Source: *https://github.com*

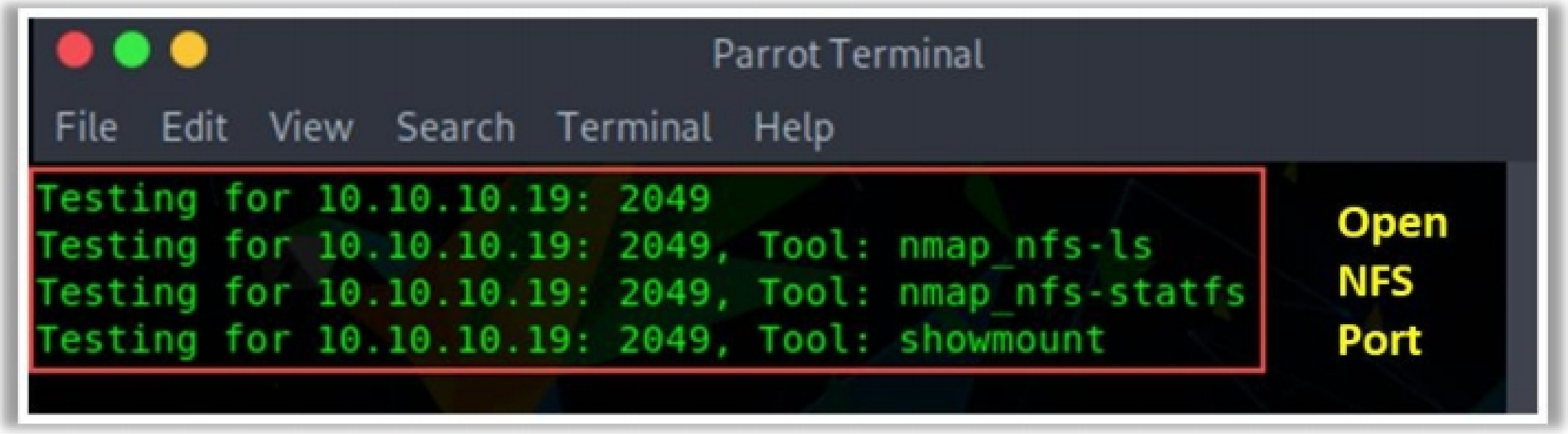
  SuperEnum includes a script that performs the basic enumeration of any open port. As shown in the screenshot, an attacker uses the `./superenum` script and then enters a text file name "`Target.txt`" having a target IP address or a list of IP addresses for enumeration.


Parrot Terminal
File Edit View Search Terminal Help
Running script
File containing target IP address

```
┌─[root@parrot]─[~]
└──╼ #cd SuperEnum
┌─[root@parrot]─[~/SuperEnum]
└──╼ #./superenum
Enter IP List filename with path
Target.txt
```

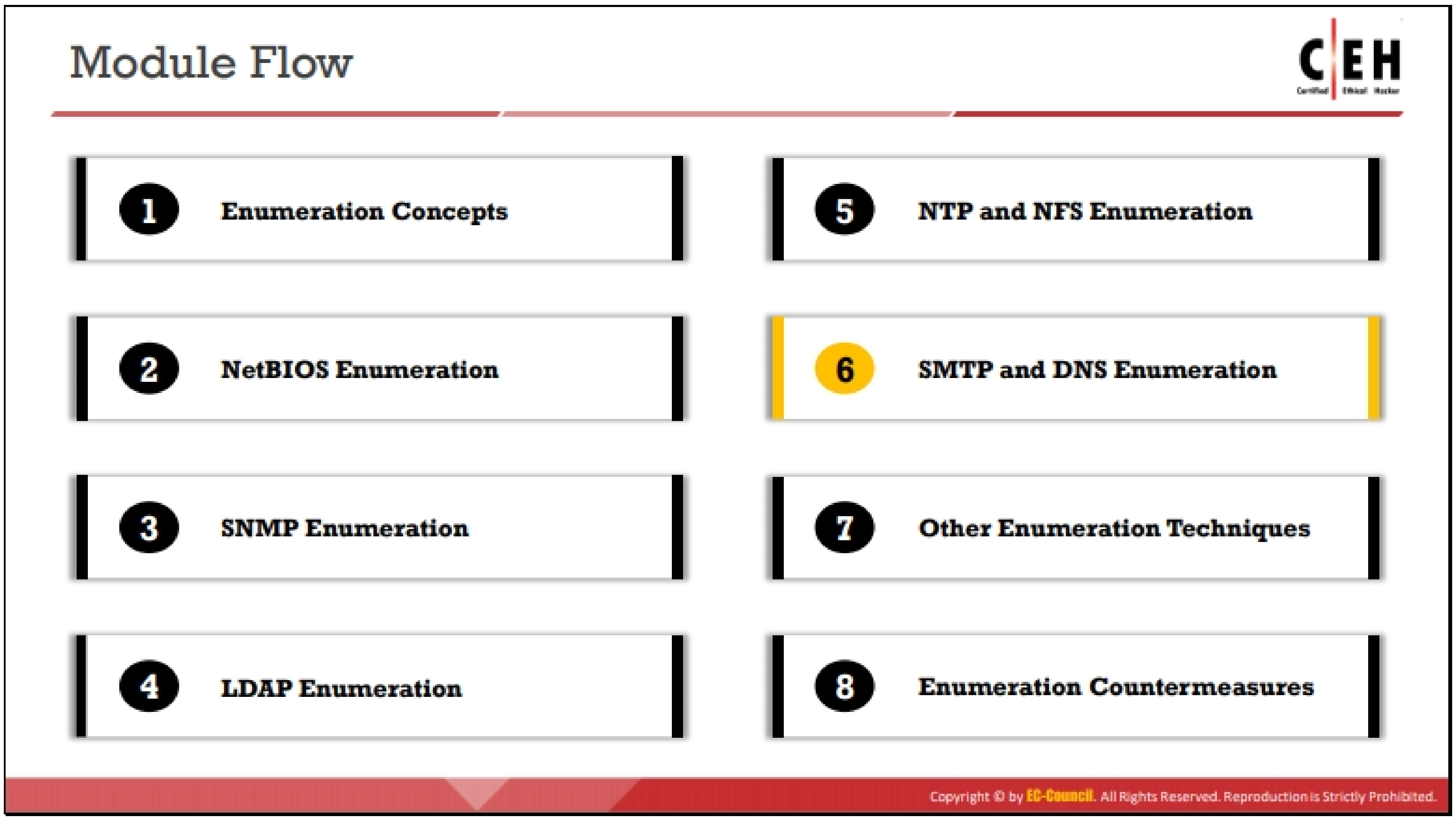
Figure 4.19: Screenshot of SuperEnum running a script

After scanning a target IP address, the script displays all the open ports, as shown in the below screenshot. Port 2049 has an NFS service running.


Parrot Terminal
File Edit View Search Terminal Help
Open
NFS
Port

```
Testing for 10.10.10.19: 2049
Testing for 10.10.10.19: 2049, Tool: nmap_nfs-ls
Testing for 10.10.10.19: 2049, Tool: nmap_nfs-statfs
Testing for 10.10.10.19: 2049, Tool: showmount
```

Figure 4.20: Screenshot of SuperEnum displaying open NFS ports

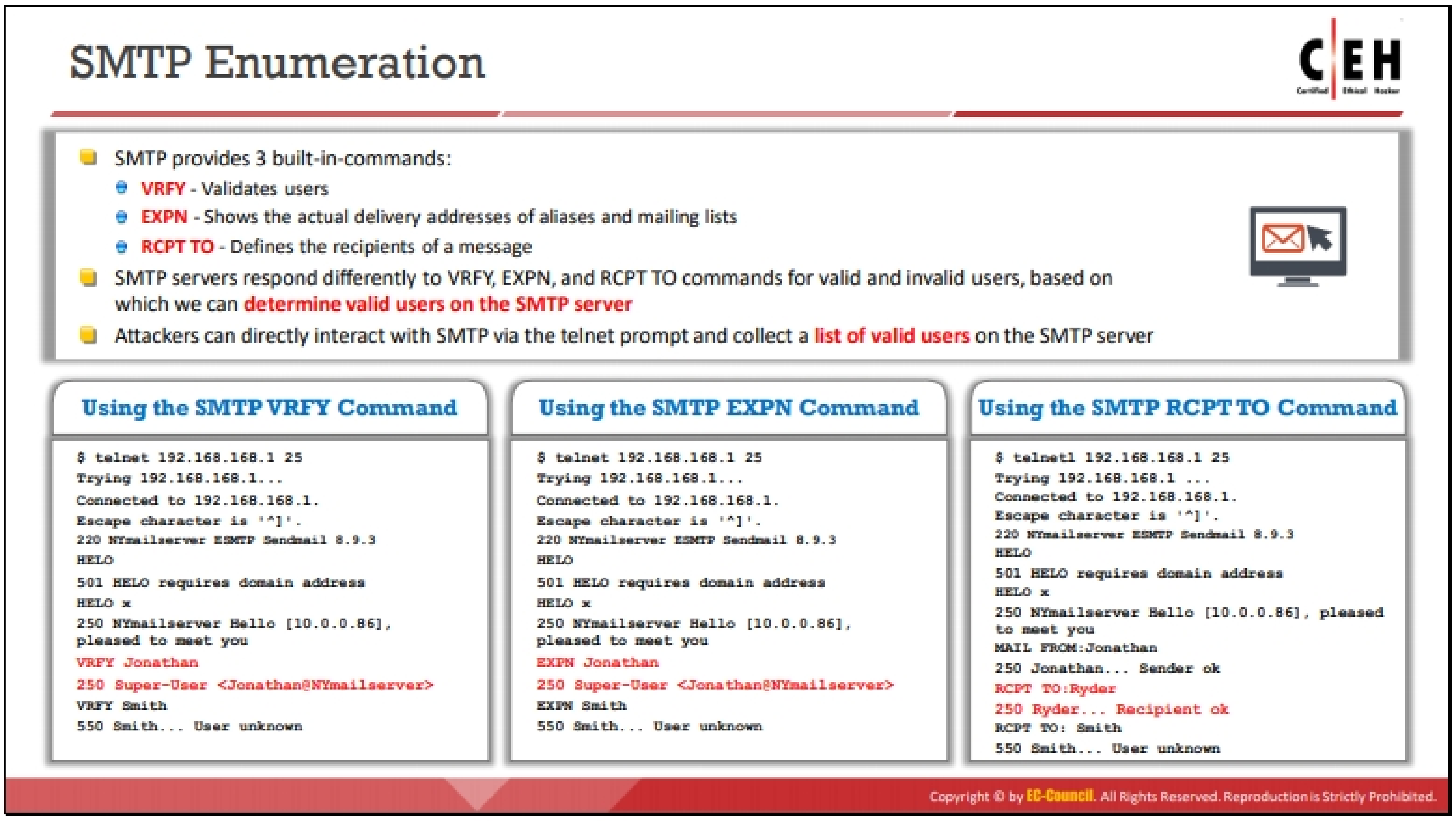


Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

SMTP and DNS Enumeration

This section describes enumeration techniques to extract information related to network resources. It also covers DNS enumeration techniques that yield information about the DNS servers and network infrastructure of the target organization. The section discusses both SMTP and DNS enumeration techniques, covering SMTP enumeration, the process of obtaining a list of valid users on an SMTP server, SMTP enumeration tools, DNS zone transfer enumeration, DNS cache snooping, and DNS zone walking.



SMTP Enumeration

- SMTP provides 3 built-in-commands:
  - **VRFY** - Validates users
  - **EXPN** - Shows the actual delivery addresses of aliases and mailing lists
  - **RCPT TO** - Defines the recipients of a message
- SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users, based on which we can **determine valid users on the SMTP server**
- Attackers can directly interact with SMTP via the telnet prompt and collect a **list of valid users** on the SMTP server

Using the SMTP VRFY Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
VRFY Jonathan
250 Super-User <Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

Using the SMTP EXPN Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
EXPN Jonathan
250 Super-User <Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

Using the SMTP RCPT TO Command

```
$ telnetl 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased
to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

SMTP Enumeration

Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS. It runs on TCP port 25, 2525, or 587.

SMTP provides the following three built-in commands.

- **VRFY:** Validates users

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
VRFY Jonathan
250 Super-User <Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

- **EXPN:** Displays the actual delivery addresses of aliases and mailing lists

  ```
  $ telnet 192.168.168.1 25
  Trying 192.168.168.1...
  Connected to 192.168.168.1.
  Escape character is '^]'.
  220 NYmailserver ESMTP Sendmail 8.9.3
  HELO
  501 HELO requires domain address
  HELO x
  250 NYmailserver Hello [10.0.0.86], pleased to meet you
  EXPN Jonathan
  250 Super-User <Jonathan@NYmailserver>
  EXPN Smith
  550 Smith... User unknown
  ```

- **RCPT TO:** Defines the recipients of the message

  ```
  $ telnetl 192.168.168.1 25
  Trying 192.168.168.1 ...
  Connected to 192.168.168.1.
  Escape character is '^]'.
  220 NYmailserver ESMTP Sendmail 8.9.3
  HELO
  501 HELO requires domain address
  HELO x
  250 NYmailserver Hello [10.0.0.86], pleased to meet you
  MAIL FROM:Jonathan
  250 Jonathan... Sender ok
  RCPT TO:Ryder
  250 Ryder... Recipient ok
  RCPT TO: Smith
  550 Smith... User unknown
  ```

SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users; therefore, valid users on the SMTP server can be determined. Attackers can directly interact with SMTP via the Telnet prompt and collect a list of valid users on the SMTP server.

Administrators and pen testers can perform SMTP enumeration using command-line utilities such as Telnet and netcat or by using tools such as Metasploit, Nmap, NetScanTools Pro, and smtp-user-enum to collect a list of valid users, delivery addresses, message recipients, etc.

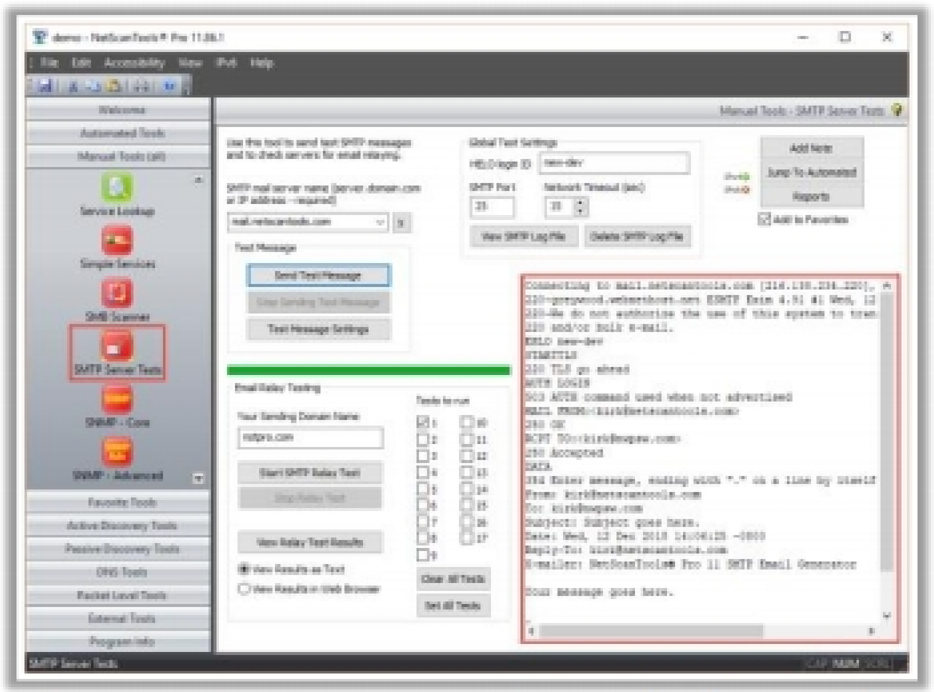
SMTP Enumeration Tools

NetScan Tools Pro

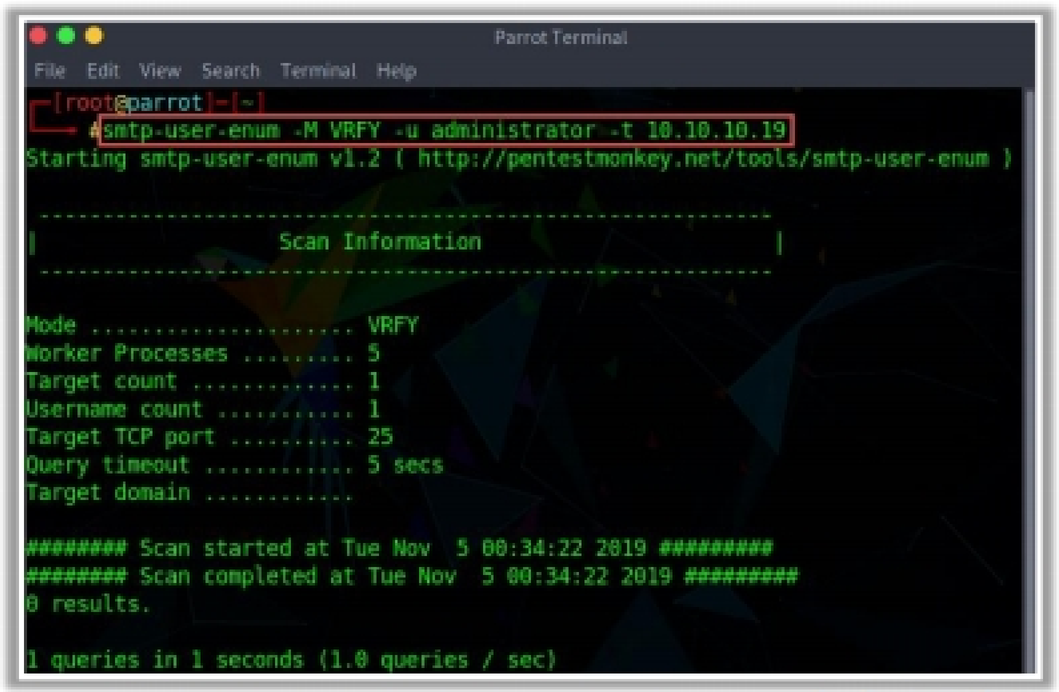
- NetScanTools Pro's SMTP Email Generator tool tests the process of sending an email message through an **SMTP server**

smtp-user-enum

- It is a tool for **enumerating OS-level user accounts** on Solaris via the SMTP service (sendmail)
- Enumeration is performed by inspecting the responses to **VRFY**, **EXPN**, and **RCPT TO** commands



https://www.netscantools.com



```
┌─[root@parrot]─[~]
└──╼ #smtp-user-enum -M VRFY -u administrator -t 10.10.10.19
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Tue Nov  5 00:34:22 2019 #########
######## Scan completed at Tue Nov  5 00:34:22 2019 #########
0 results.

1 queries in 1 seconds (1.0 queries / sec)
```

http://pentestmonkey.net

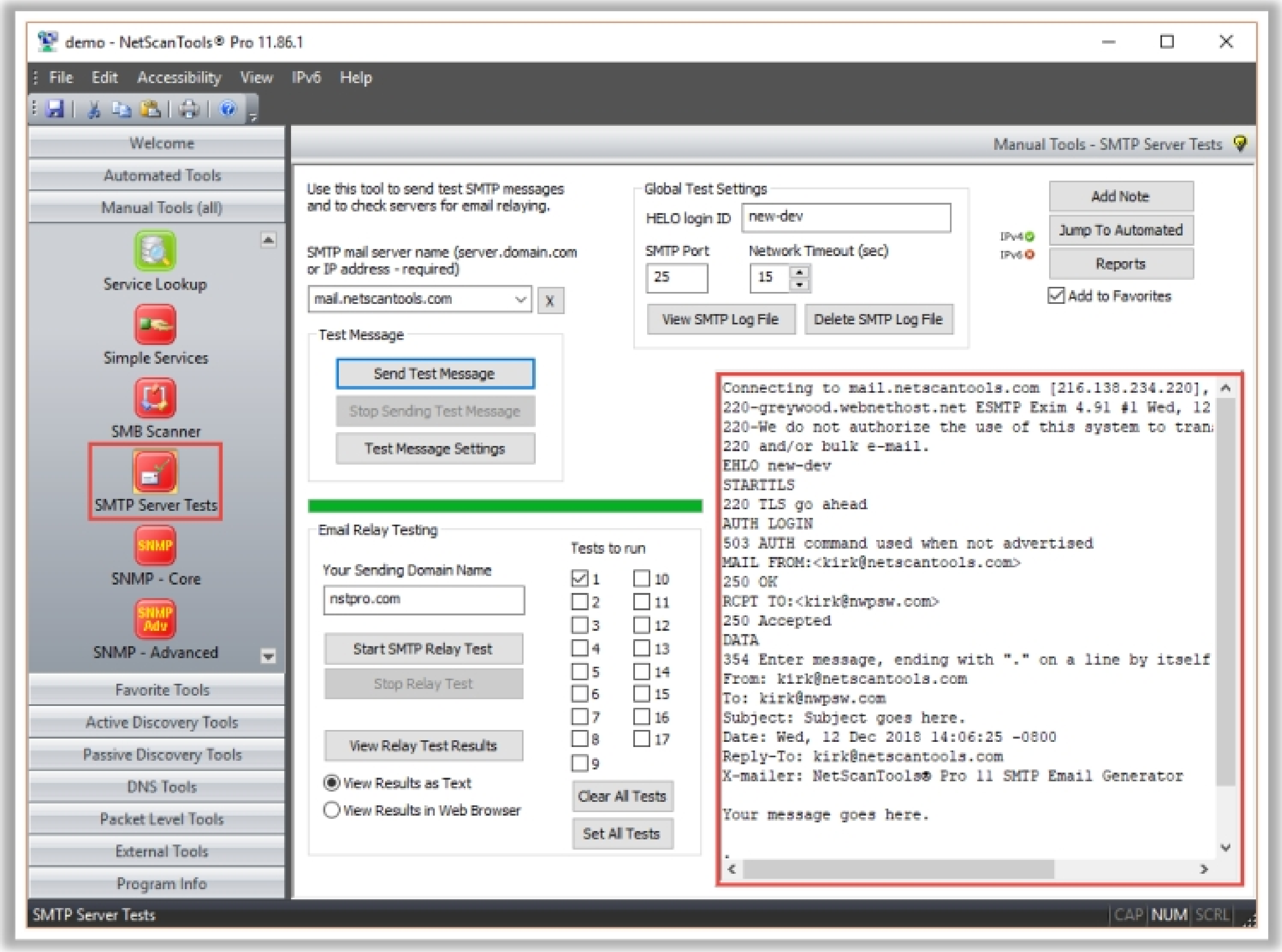
SMTP Enumeration Tools

SMTP enumeration tools are used to perform username enumeration. Attackers can use the usernames obtained from this enumeration to launch further attacks on other systems in the network.

- **NetScanTools Pro**

  Source: *https://www.netscantools.com*

  NetScanTools Pro's SMTP Email Generator tool tests the process of sending an email message through an SMTP server. Attackers use NetScanTools Pro for SMTP enumeration and extract all the email header parameters, including confirm/urgent flags. Attackers can also record the email session in a log file and then view the communications between NetScanTools Pro and the SMTP server in the log file.


demo - NetScanTools® Pro 11.86.1
File
Edit
Accessibility
View
IPv6
Help
Welcome
Automated Tools
Manual Tools (all)
Service Lookup
Simple Services
SMB Scanner
SMTP Server Tests
SNMP - Core
SNMP - Advanced
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Program Info
Manual Tools - SMTP Server Tests
Global Test Settings
View SMTP Log File
Delete SMTP Log File
Add Note
Jump To Automated
Reports
☑ Add to Favorites
IPv4
IPv6
Test Message
Send Test Message
Stop Sending Test Message
Test Message Settings
Email Relay Testing
Tests to run
Start SMTP Relay Test
Stop Relay Test
View Relay Test Results
● View Results as Text
○ View Results in Web Browser
☑ 1
☐ 2
☐ 3
☐ 4
☐ 5
☐ 6
☐ 7
☐ 8
☐ 9
☐ 10
☐ 11
☐ 12
☐ 13
☐ 14
☐ 15
☐ 16
☐ 17
Clear All Tests
Set All Tests
SMTP Server Tests
CAP
NUM
SCRL

Use this tool to send test SMTP messages and to check servers for email relaying.

SMTP mail server name (server.domain.com or IP address - required): mail.netscantools.com

HELO login ID: new-dev

SMTP Port: 25

Network Timeout (sec): 15

Your Sending Domain Name: nstpro.com

```
Connecting to mail.netscantools.com [216.138.234.220],
220-greywood.webnethost.net ESMTP Exim 4.91 #1 Wed, 12
220-We do not authorize the use of this system to tran
220 and/or bulk e-mail.
EHLO new-dev
STARTTLS
220 TLS go ahead
AUTH LOGIN
503 AUTH command used when not advertised
MAIL FROM:<kirk@netscantools.com>
250 OK
RCPT TO:<kirk@nwpsw.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: kirk@netscantools.com
To: kirk@nwpsw.com
Subject: Subject goes here.
Date: Wed, 12 Dec 2018 14:06:25 -0800
Reply-To: kirk@netscantools.com
X-mailer: NetScanTools® Pro 11 SMTP Email Generator

Your message goes here.

.
```

Figure 4.21: Screenshot of NetScanTools Pro

- **smtp-user-enum**

  Source: *http://pentestmonkey.net*

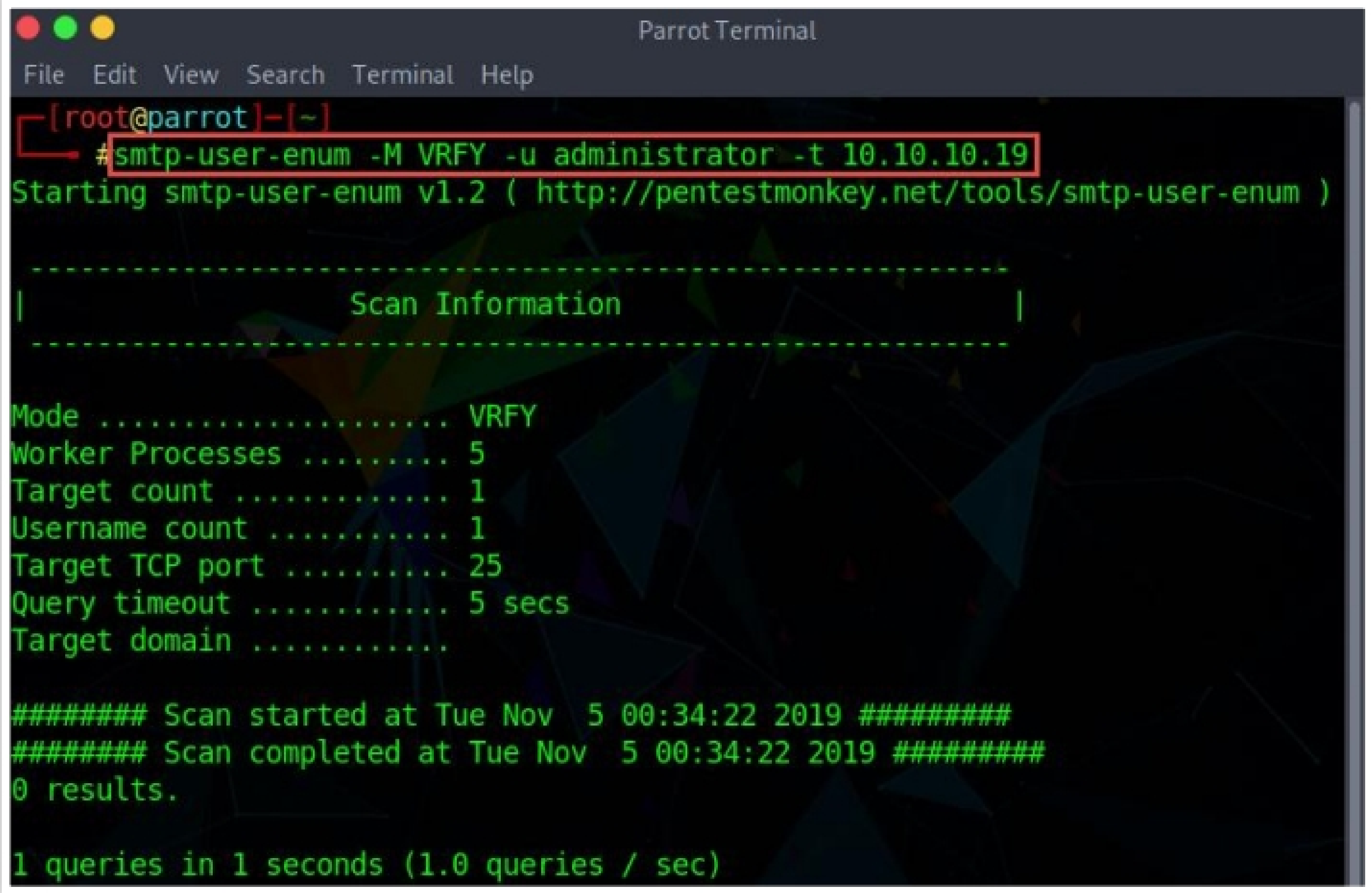
  smtp-user-enum is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail). Enumeration is performed by inspecting the responses to VRFY, EXPN, and RCPT TO commands. As shown in the screenshot, smtp-user-enum needs to be passed on to a list of users and at least one target running an SMTP service. The syntax for using smtp-user-enum is as follows:

  `smtp-user-enum.pl [options] (-u username|-U file-of-usernames) (-t host|-T file-of-targets)`

  smtp-user-enum has the following options:

  - **-m n**: Maximum number of processes (default: 5)
  - **-M mode**: Specify the SMTP command to use for username guessing from among EXPN, VRFY, and RCPT TO (default: VRFY)
  - **-u user**: Check if a user exists on the remote system
  - **-f addr**: Specify the from email address to use for "RCPT TO" guessing (default: user@example.com)

- **-D dom**: Specify the domain to append to the supplied user list to create email addresses (default: none)
- **-U file**: Select the file containing usernames to check via the SMTP service
- **-t host**: Specify the server host running the SMTP service
- **-T file**: Select the file containing hostnames running the SMTP service
- **-p port**: Specify the TCP port on which the SMTP service runs (default: 25)
- **-d**: Debugging output
- **-t n**: Wait for a maximum of n seconds for the reply (default: 5)
- **-v**: Verbose
- **-h**: Help message



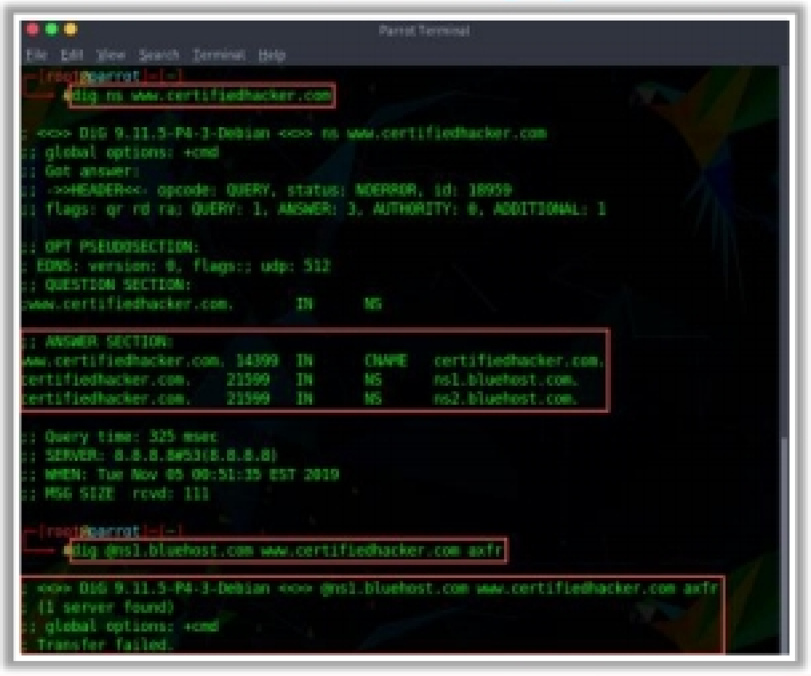
```
┌─[root@parrot]─[~]
└──╼ #smtp-user-enum -M VRFY -u administrator -t 10.10.10.19
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Tue Nov  5 00:34:22 2019 #########
######## Scan completed at Tue Nov  5 00:34:22 2019 #########
0 results.

1 queries in 1 seconds (1.0 queries / sec)
```

Figure 4.22: Screenshot of smtp-user-enum

DNS Enumeration Using Zone Transfer

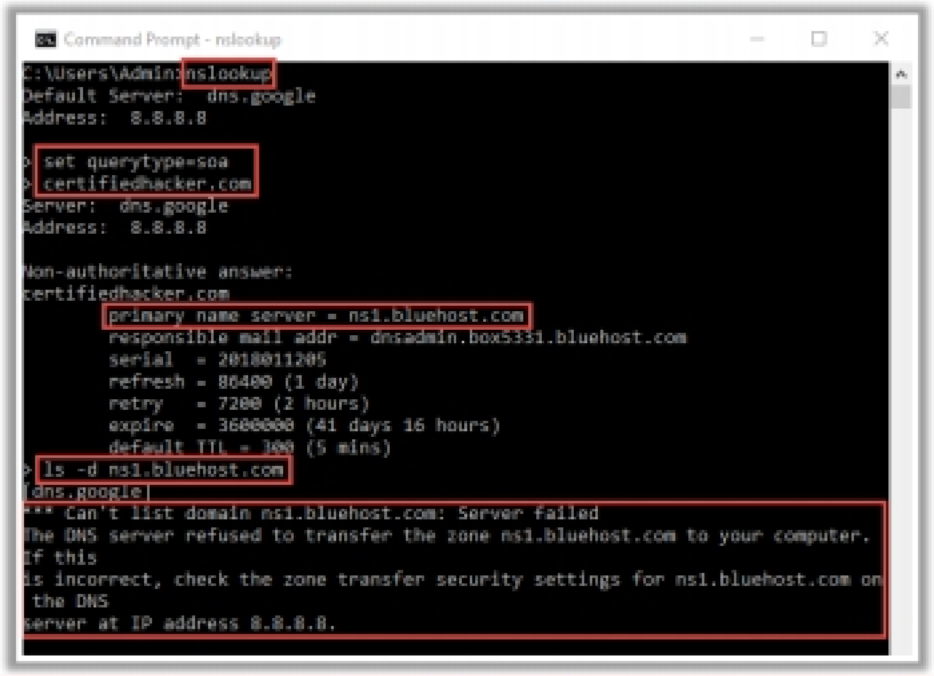
- If the target DNS server allows zone transfers, then attackers use this technique to obtain **DNS server names**, **hostnames**, **machine names**, **usernames**, **IP addresses**, **aliases**, etc. assigned within a target domain
- Attackers perform DNS zone transfer using tools, such as **nslookup**, **dig**, and **DNSRecon**; if DNS transfer setting is enabled on the target name server, it will provide DNS information, or else it will return an error saying it has failed or refuses the zone transfer

Linux DNS zone transfer using dig command



```
┌─[root@parrot]─[~]
└──╼ #dig ns www.certifiedhacker.com

; <<>> DiG 9.11.5-P4-3-Debian <<>> ns www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18959
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.       IN      NS

;; ANSWER SECTION:
www.certifiedhacker.com. 14399  IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    21599   IN      NS      ns1.bluehost.com.
certifiedhacker.com.    21599   IN      NS      ns2.bluehost.com.

;; Query time: 325 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Nov 05 00:51:35 EST 2019
;; MSG SIZE  rcvd: 111

┌─[root@parrot]─[~]
└──╼ #dig @ns1.bluehost.com www.certifiedhacker.com axfr

; <<>> DiG 9.11.5-P4-3-Debian <<>> @ns1.bluehost.com www.certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

Windows DNS zone transfer using nslookup command



```
C:\Users\Admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set querytype=soa
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
certifiedhacker.com
        primary name server = ns1.bluehost.com
        responsible mail addr = dnsadmin.box5331.bluehost.com
        serial  = 2018011205
        refresh = 86400 (1 day)
        retry   = 7200 (2 hours)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
> ls -d ns1.bluehost.com
[dns.google]
*** Can't list domain ns1.bluehost.com: Server failed
The DNS server refused to transfer the zone ns1.bluehost.com to your computer. If this
is incorrect, check the zone transfer security settings for ns1.bluehost.com on the DNS
server at IP address 8.8.8.8.
```

DNS Enumeration Using Zone Transfer

DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. In most cases, the primary DNS server maintains a backup or secondary server for redundancy, which holds all the information stored in the primary server. The DNS server uses zone transfer to distribute changes made to the main server to the secondary server(s). An attacker performs DNS zone transfer enumeration to locate the DNS server and access records of the target organization. If the DNS server of the target organization allows zone transfers, then attackers can perform DNS zone transfer to obtain DNS server names, hostnames, machine names, usernames, IP addresses, aliases, etc. assigned within a target domain.

In DNS enumeration using zone transfer, an attacker attempts to retrieve a copy of the entire zone file for a domain from the DNS server. Attackers can perform DNS zone transfer using tools such as nslookup, dig command, and DNSRecon. If the DNS transfer setting is enabled on the target name server, it will provide the DNS information; else, it will return an error stating it has failed or refused the zone transfer.

To perform a DNS zone transfer, the attacker sends a zone-transfer request to the DNS server pretending to be a client; the DNS server then sends a portion of its database as a zone to the attacker. This zone may contain a large amount of information about the DNS zone network.

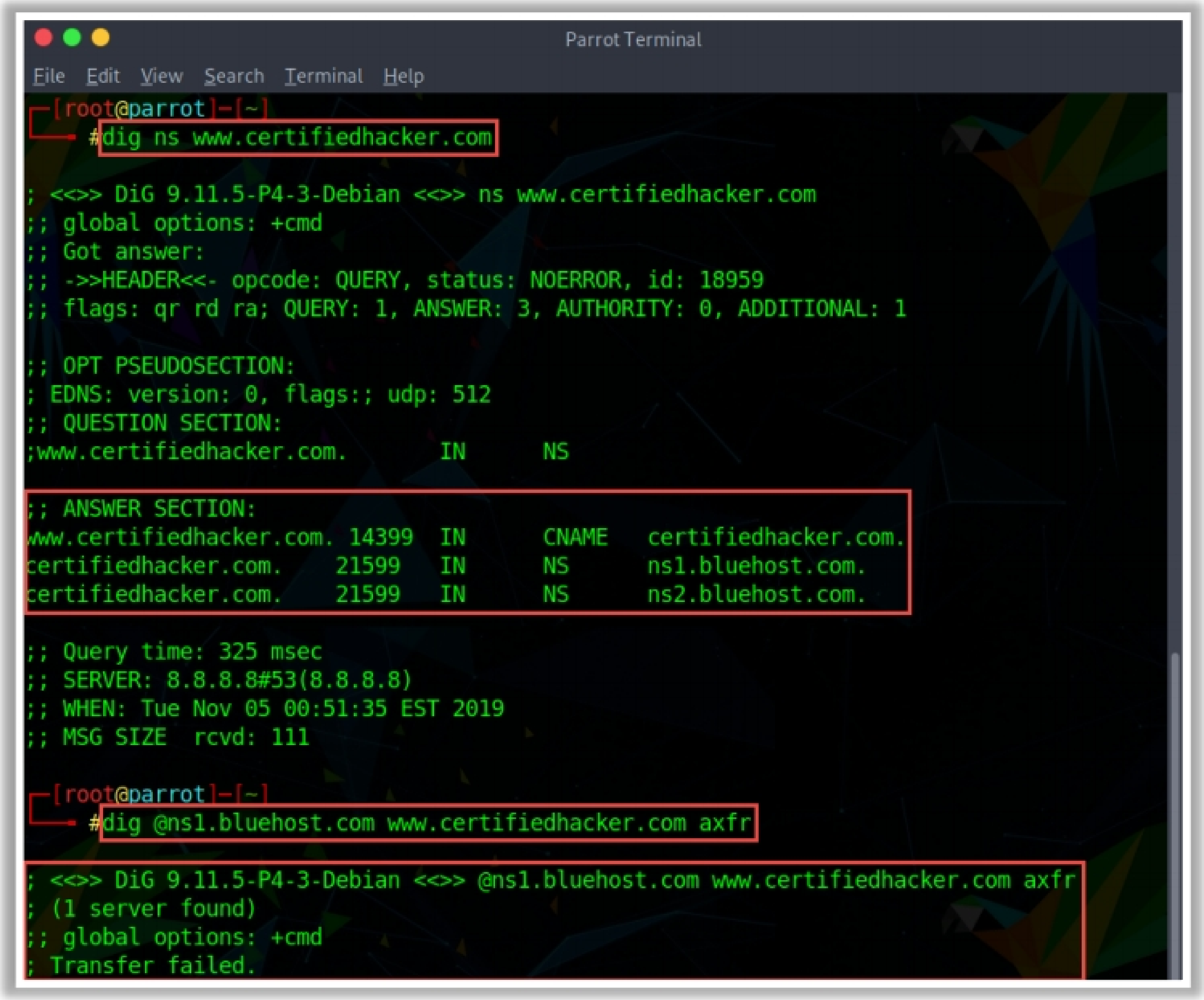
- **dig Command**

  Attackers use the `dig` command on Linux-based systems to query the DNS name servers and retrieve information about the target host addresses, name servers, mail exchanges, etc. As shown in the screenshot, attackers use the following command to perform DNS zone transfer:

  `dig ns <target domain>`

  The above command retrieves all the DNS name servers of the target domain. Next, attackers use one of the name servers from the output of the above command to test whether the target DNS allows zone transfers. They use the following command for this purpose:

  `dig @<domain of name server> <target domain> axfr`



```
┌─[root@parrot]─[~]
└──╼ #dig ns www.certifiedhacker.com

; <<>> DiG 9.11.5-P4-3-Debian <<>> ns www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18959
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.       IN      NS

;; ANSWER SECTION:
ww.certifiedhacker.com. 14399   IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    21599   IN      NS      ns1.bluehost.com.
certifiedhacker.com.    21599   IN      NS      ns2.bluehost.com.

;; Query time: 325 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Nov 05 00:51:35 EST 2019
;; MSG SIZE  rcvd: 111

┌─[root@parrot]─[~]
└──╼ #dig @ns1.bluehost.com www.certifiedhacker.com axfr

; <<>> DiG 9.11.5-P4-3-Debian <<>> @ns1.bluehost.com www.certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

Figure 4.23: Screenshot of Linux DNS zone transfer using dig command

- **nslookup Command**

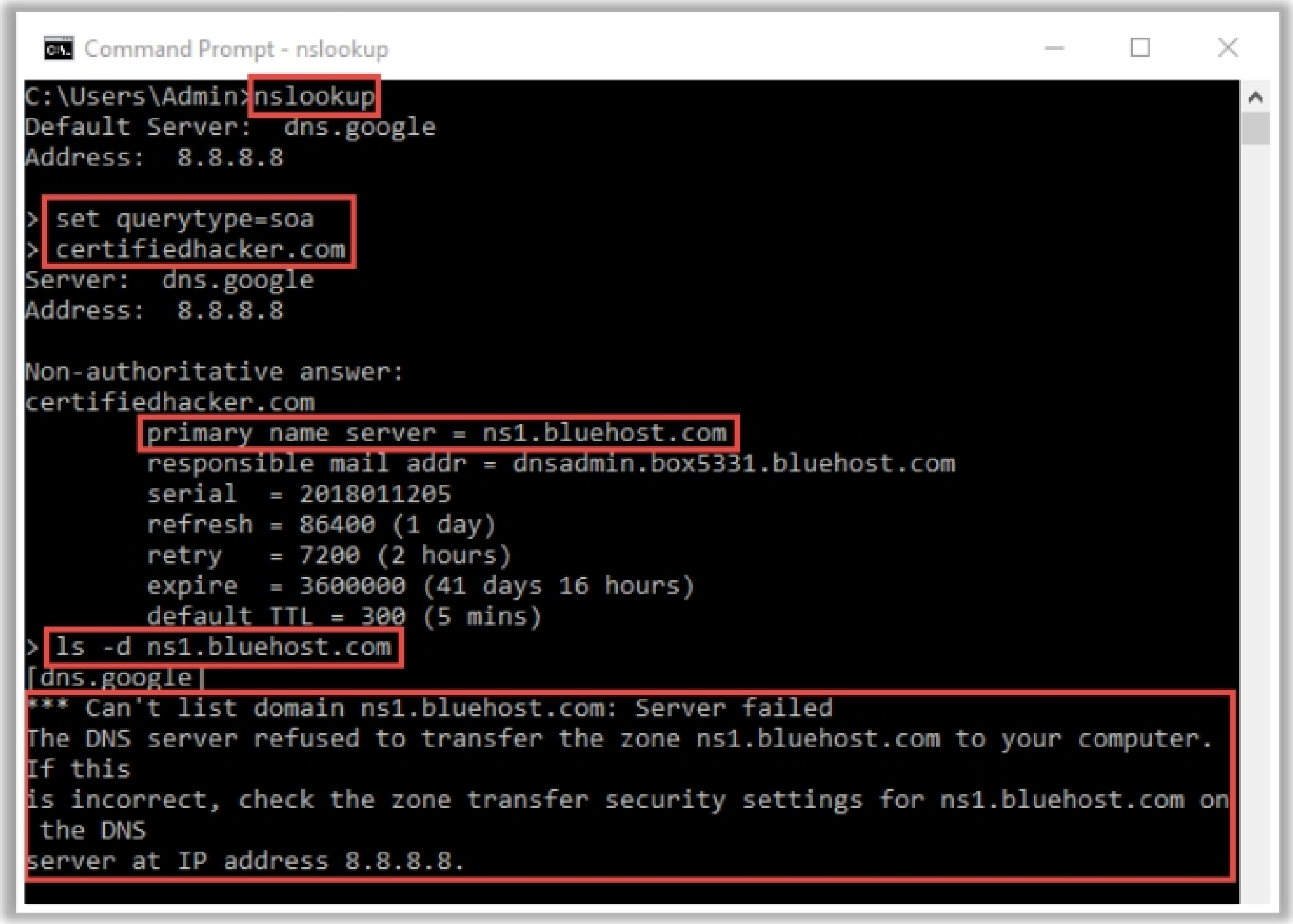
  Source: *https://docs.microsoft.com*

  Attackers use the nslookup command on Windows-based systems to query the DNS name servers and retrieve information about the target host addresses, name servers, mail exchanges, etc. As shown in the screenshot, attackers use the following command to perform DNS zone transfer:

  ```
  nslookup
  set querytype=soa
  <target domain>
  ```

  The above command sets the query type to the Start of Authority (SOA) record to retrieve administrative information about the DNS zone of the target domain **`certifiedhacker.com`**. The following command is used to attempt to transfer the zone of the specified name server:

  ```
  /ls -d <domain of name server>
  ```



```
C:\Users\Admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set querytype=soa
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
certifiedhacker.com
        primary name server = ns1.bluehost.com
        responsible mail addr = dnsadmin.box5331.bluehost.com
        serial  = 2018011205
        refresh = 86400 (1 day)
        retry   = 7200 (2 hours)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
> ls -d ns1.bluehost.com
[dns.google]
*** Can't list domain ns1.bluehost.com: Server failed
The DNS server refused to transfer the zone ns1.bluehost.com to your computer.
If this
is incorrect, check the zone transfer security settings for ns1.bluehost.com on
 the DNS
server at IP address 8.8.8.8.
```

Figure 4.24: Screenshot of Windows DNS zone transfer using the nslookup command

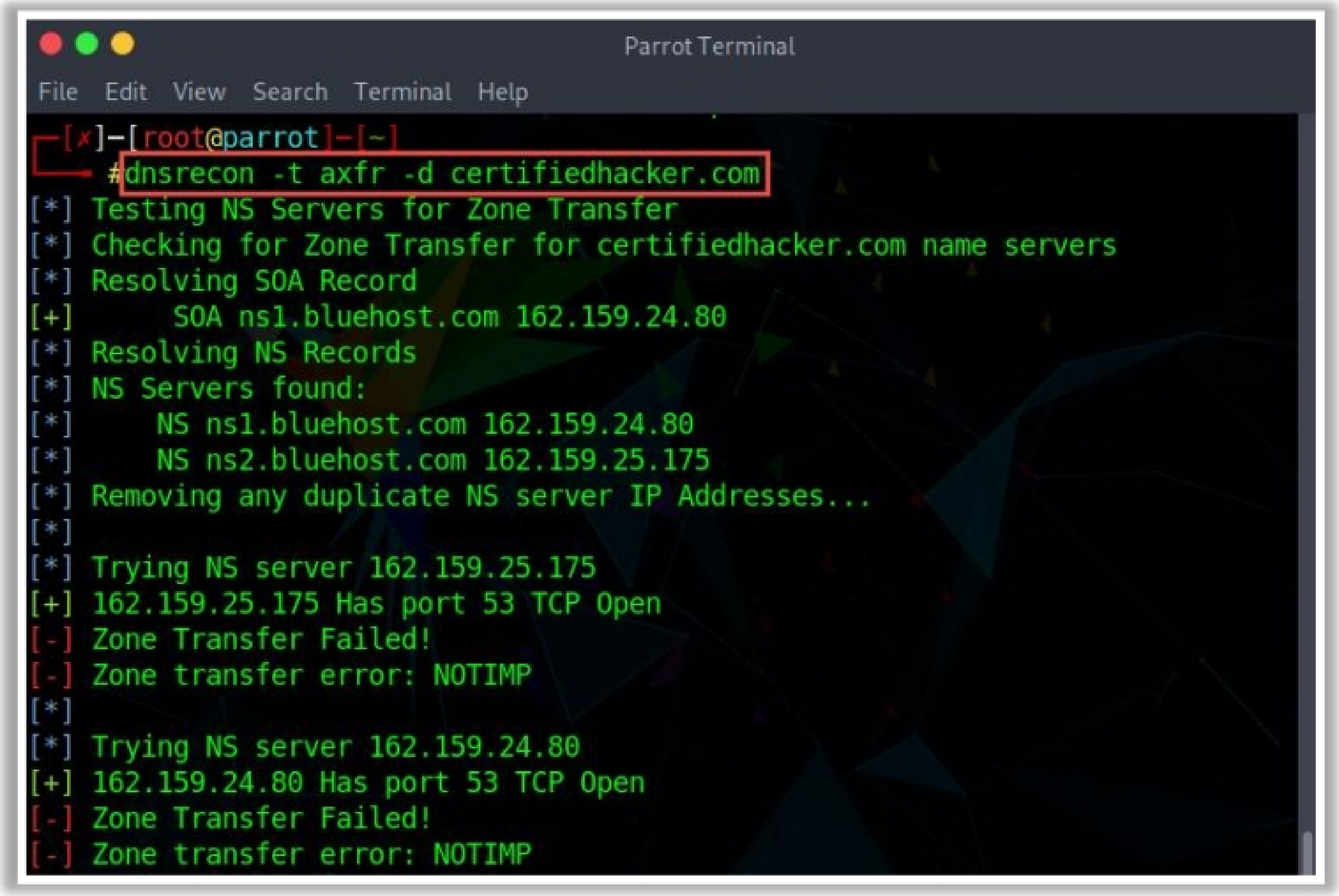
- **DNSRecon**

  Source: *https://github.com*

  Attackers use DNSRecon to check all NS records of the target domain for zone transfers. As shown in the screenshot, attackers use the following command for DNS zone transfer:

  `dnsrecon -t axfr -d <target domain>`

  In the above command, the -t option specifies the type of enumeration to be performed, axfr is the type of enumeration in which all NS servers are tested for a zone transfer, and the -d option specifies the target domain.



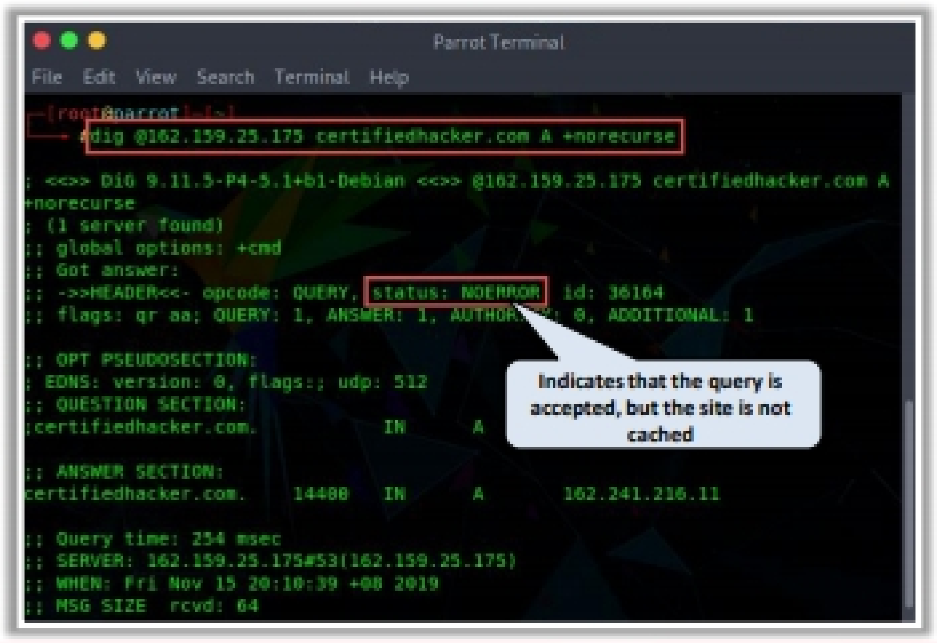
```
┌─[x]─[root@parrot]─[~]
└──╼ #dnsrecon -t axfr -d certifiedhacker.com
[*] Testing NS Servers for Zone Transfer
[*] Checking for Zone Transfer for certifiedhacker.com name servers
[*] Resolving SOA Record
[+]      SOA ns1.bluehost.com 162.159.24.80
[*] Resolving NS Records
[*] NS Servers found:
[*]     NS ns1.bluehost.com 162.159.24.80
[*]     NS ns2.bluehost.com 162.159.25.175
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 162.159.25.175
[+] 162.159.25.175 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] Zone transfer error: NOTIMP
[*]
[*] Trying NS server 162.159.24.80
[+] 162.159.24.80 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] Zone transfer error: NOTIMP
```

Figure 4.25: Screenshot of DNS zone transfer using DNSRecon

DNS Cache Snooping

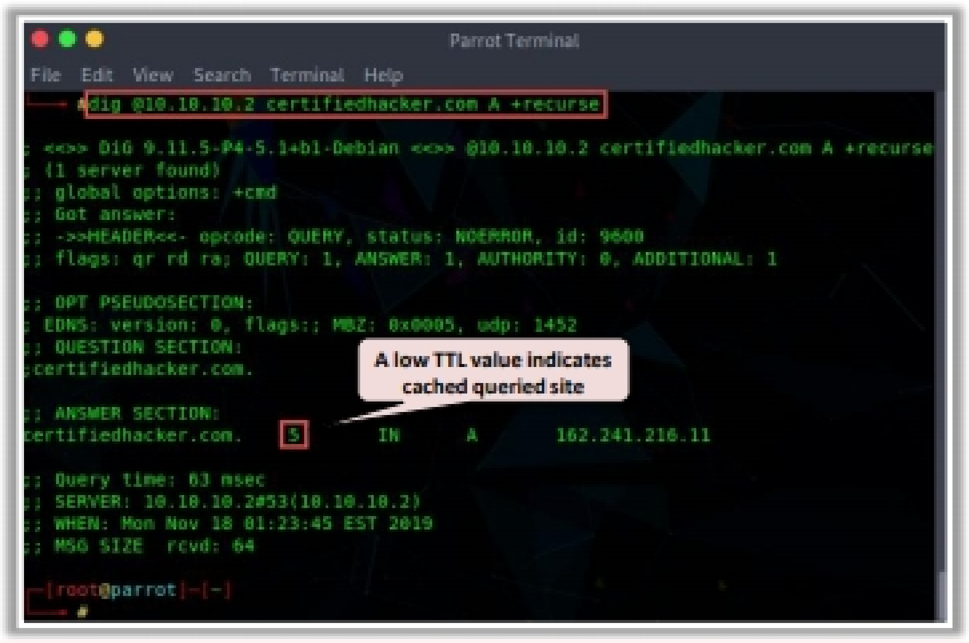
- DNS cache snooping is a **DNS enumeration** technique whereby an **attacker queries** the **DNS server** for a specific cached DNS record

Non-recursive Method	Attackers send a **non-recursive query** by setting the **Recursion Desired** (RD) bit in the query header to zero
Recursive Method	Attackers send a recursive query to **determine the time** the **DNS record** resides in the cache



```
┌─[root@parrot]─[~]
└──╼ #dig @162.159.25.175 certifiedhacker.com A +norecurse

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @162.159.25.175 certifiedhacker.com A
+norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36164
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;certifiedhacker.com.           IN      A

;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      A       162.241.216.11

;; Query time: 254 msec
;; SERVER: 162.159.25.175#53(162.159.25.175)
;; WHEN: Fri Nov 15 20:10:39 +08 2019
;; MSG SIZE  rcvd: 64
```

Indicates that the query is accepted, but the site is not cached



```
└──╼ #dig @10.10.10.2 certifiedhacker.com A +recurse

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @10.10.10.2 certifiedhacker.com A +recurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9600
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1452
;; QUESTION SECTION:
;certifiedhacker.com.

;; ANSWER SECTION:
certifiedhacker.com.    5       IN      A       162.241.216.11

;; Query time: 63 msec
;; SERVER: 10.10.10.2#53(10.10.10.2)
;; WHEN: Mon Nov 18 01:23:45 EST 2019
;; MSG SIZE  rcvd: 64

┌─[root@parrot]─[~]
└──╼ #
```

A low TTL value indicates cached queried site

DNS Cache Snooping

DNS cache snooping is a type of DNS enumeration technique in which an attacker queries the DNS server for a specific cached DNS record. By using this cached record, the attacker can determine the sites recently visited by the user. This information can further reveal important information such as the name of the owner of the DNS server, its service provider, the name of its vendor, and bank details. By using this information, the attacker can perform a social engineering attack on the target user. Attackers perform DNS cache snooping using various tools such as the dig command, DNS Snoop Dogg, and DNSRecon.

Attackers use the following two DNS cache snooping methods to snoop on a target domain.

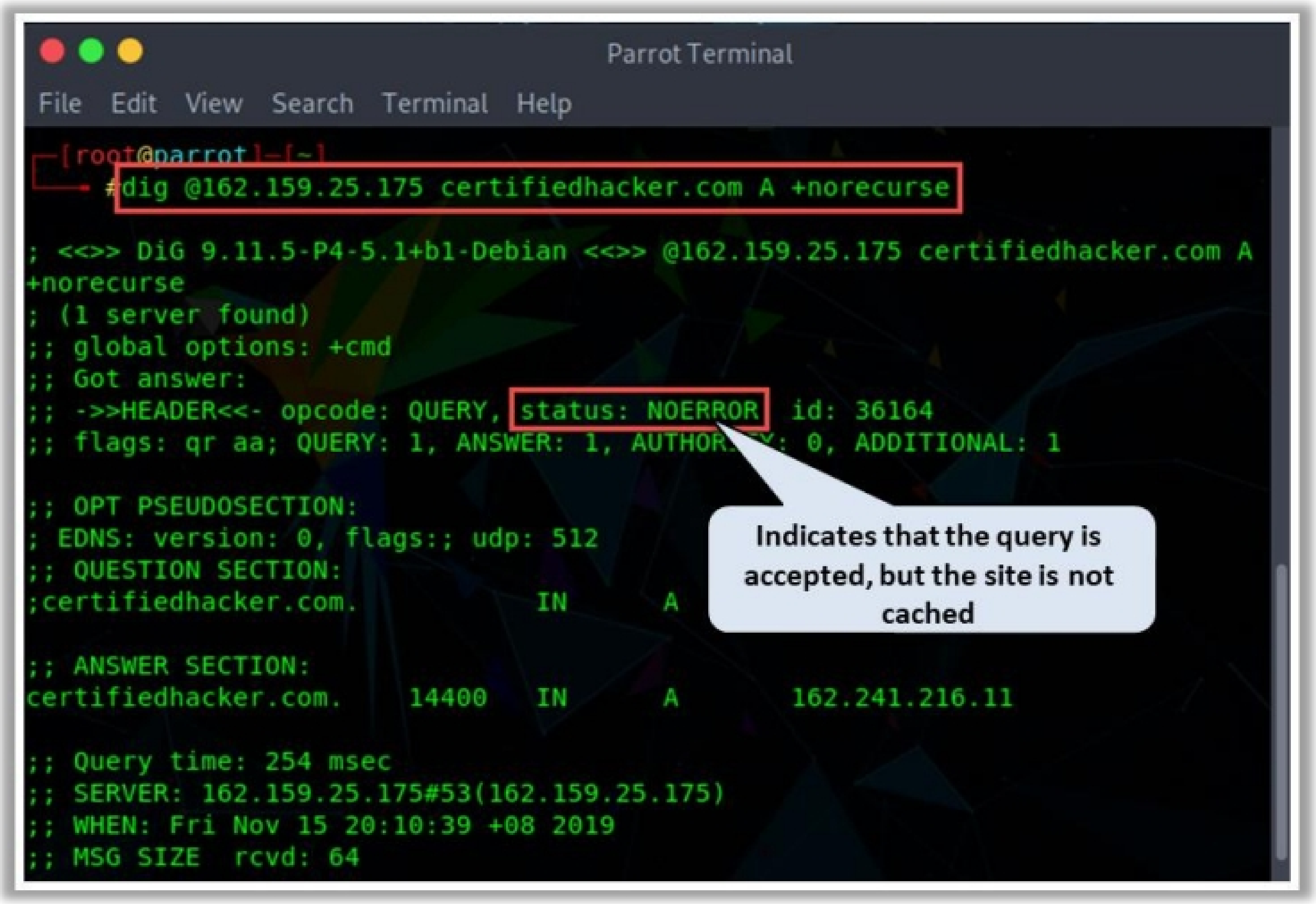
- **Non-recursive Method**

  In this method, to snoop on a DNS server, attackers send a non-recursive query by setting the Recursion Desired (RD) bit in the query header to zero. Attackers query the DNS cache for a specific DNS record such as A, CNAME, PTR, CERT, SRV, and MX. If the queried record is present in the DNS cache, the DNS server responds with the information indicating that some user on the system has visited a specific domain. Otherwise, the DNS server responds with the information about another DNS server that can return an answer to the query, or it replies with the `root.hints` file containing information about all root DNS servers.

  Attackers use the `dig` command followed by the name/IP address of the DNS server, domain name, and type of DNS record file. The `+norecurse` option is used to set the query to non-recursive.

  ```
  dig @<IP of DNS server> <Target domain> A +norecurse
  ```

As shown in the screenshot, the status **`NOERROR`** implies that the query was accepted but no answer was returned, thereby indicating that no user from the system had visited the queried site.



```
┌─[root@parrot]─[~]
└──╼ #dig @162.159.25.175 certifiedhacker.com A +norecurse

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @162.159.25.175 certifiedhacker.com A
+norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36164
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;certifiedhacker.com.           IN      A

;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      A       162.241.216.11

;; Query time: 254 msec
;; SERVER: 162.159.25.175#53(162.159.25.175)
;; WHEN: Fri Nov 15 20:10:39 +08 2019
;; MSG SIZE  rcvd: 64
```

Indicates that the query is accepted, but the site is not cached

Figure 4.26: Screenshot of a dig query for a site that is not cached

- **Recursive Method**

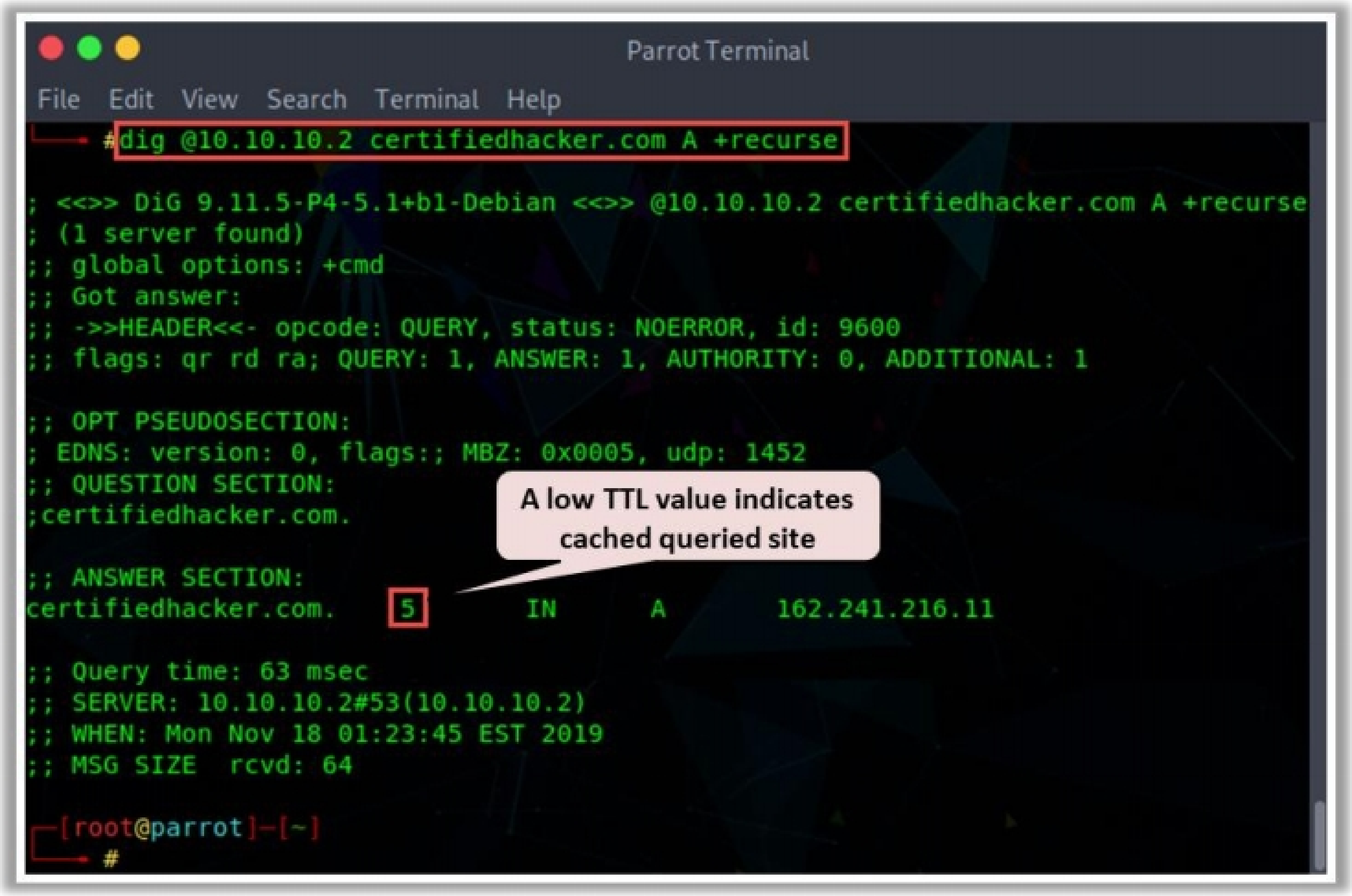
  In this method, to snoop on the DNS server, attackers send a recursive query by setting the **`+recurse`** option instead of the **`+norecurse`** option. Similar to the non-recursive method, the attackers query the DNS cache for a specific DNS record such as A, CNAME, PTR, CERT, SRV, and MX.

  In this method, the time-to-live (TTL) field is examined to determine the duration for which the DNS record remains in the cache. Here, the TTL value obtained from the result is compared with the TTL that was initially set in the TTL field. If the TTL value in the result is less than the initial TTL value, the record is cached, indicating that someone on the system has visited that site. However, if the queried record were not present in the cache, it will be added to the cache after the first query is sent.

  Attackers use the same **`dig`** command as in the non-recursive method but with the **`+recurse`** option instead of the **`+norecurse`** option:

  `dig @<IP of DNS server> <Target domain> A +recurse`

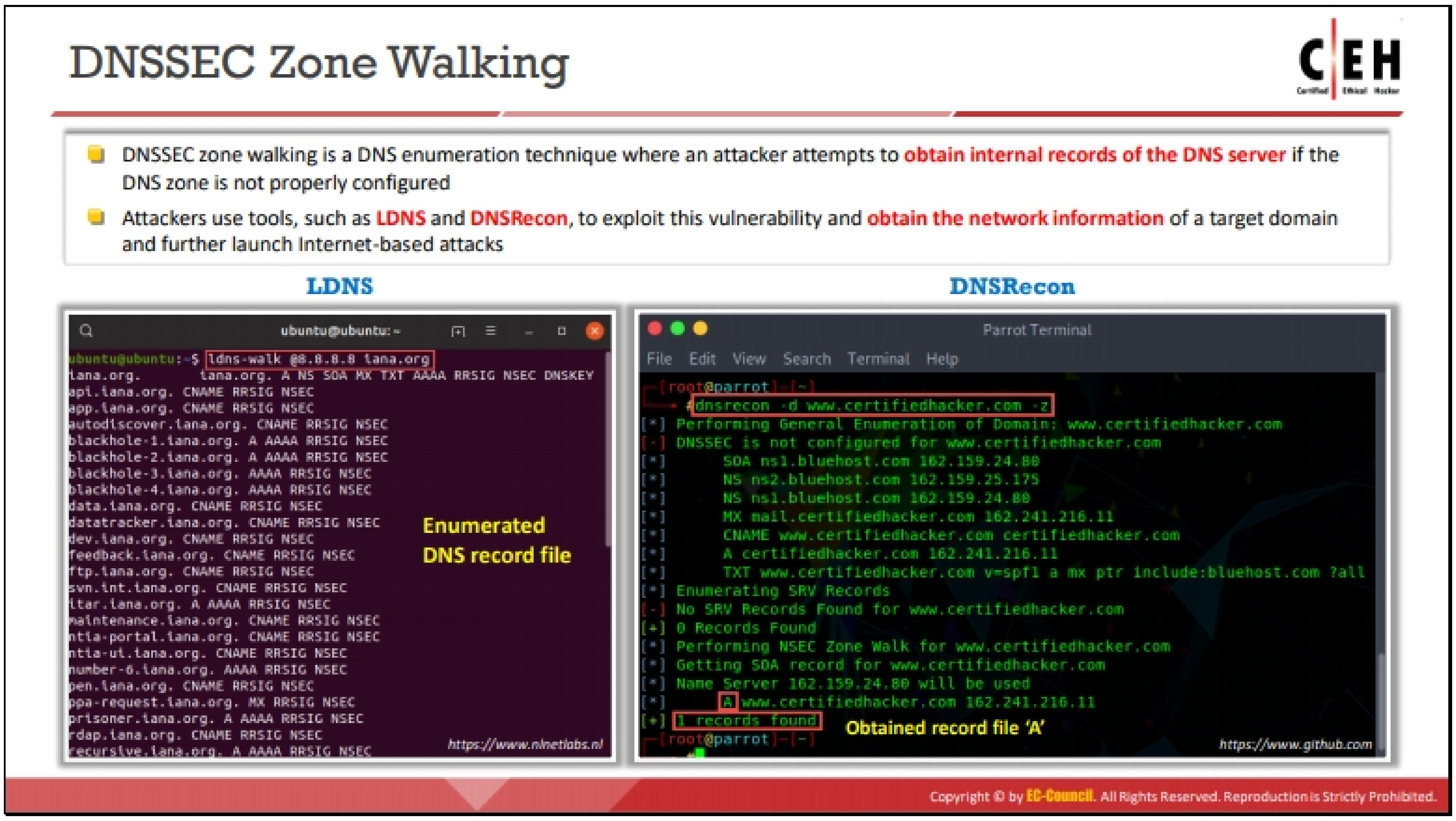
As shown in the screenshot, the TTL value for the domain `certifiedhacker.com` is considerably low, which strongly suggests that the domain was already in the cache when the query was issued.



```
└──╼ #dig @10.10.10.2 certifiedhacker.com A +recurse

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @10.10.10.2 certifiedhacker.com A +recurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9600
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1452
;; QUESTION SECTION:
;certifiedhacker.com.

;; ANSWER SECTION:
certifiedhacker.com.    5       IN      A       162.241.216.11

;; Query time: 63 msec
;; SERVER: 10.10.10.2#53(10.10.10.2)
;; WHEN: Mon Nov 18 01:23:45 EST 2019
;; MSG SIZE  rcvd: 64

┌─[root@parrot]─[~]
└──╼ #
```

A low TTL value indicates cached queried site

Figure 4.27: Screenshot of a dig query for a cached site



DNSSEC Zone Walking

- DNSSEC zone walking is a DNS enumeration technique where an attacker attempts to **obtain internal records of the DNS server** if the DNS zone is not properly configured
- Attackers use tools, such as **LDNS** and **DNSRecon**, to exploit this vulnerability and **obtain the network information** of a target domain and further launch Internet-based attacks

LDNS

```
ubuntu@ubuntu:~$ ldns-walk @8.8.8.8 iana.org
iana.org.       iana.org. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY
api.iana.org. CNAME RRSIG NSEC
app.iana.org. CNAME RRSIG NSEC
autodiscover.iana.org. CNAME RRSIG NSEC
blackhole-1.iana.org. A AAAA RRSIG NSEC
blackhole-2.iana.org. A AAAA RRSIG NSEC
blackhole-3.iana.org. AAAA RRSIG NSEC
blackhole-4.iana.org. AAAA RRSIG NSEC
data.iana.org. CNAME RRSIG NSEC
datatracker.iana.org. CNAME RRSIG NSEC
dev.iana.org. CNAME RRSIG NSEC
feedback.iana.org. CNAME RRSIG NSEC
ftp.iana.org. CNAME RRSIG NSEC
svn.int.iana.org. CNAME RRSIG NSEC
itar.iana.org. A AAAA RRSIG NSEC
maintenance.iana.org. CNAME RRSIG NSEC
ntia-portal.iana.org. CNAME RRSIG NSEC
ntia-ui.iana.org. CNAME RRSIG NSEC
number-6.iana.org. AAAA RRSIG NSEC
pen.iana.org. CNAME RRSIG NSEC
ppa-request.iana.org. MX RRSIG NSEC
prisoner.iana.org. A AAAA RRSIG NSEC
rdap.iana.org. CNAME RRSIG NSEC
recursive.iana.org. A AAAA RRSIG NSEC
```

Enumerated DNS record file

https://www.nlnetlabs.nl

DNSRecon

```
┌─[root@parrot]─[~]
└──╼ #dnsrecon -d www.certifiedhacker.com -z
[*] Performing General Enumeration of Domain: www.certifiedhacker.com
[-] DNSSEC is not configured for www.certifiedhacker.com
[*]      SOA ns1.bluehost.com 162.159.24.80
[*]      NS ns2.bluehost.com 162.159.25.175
[*]      NS ns1.bluehost.com 162.159.24.80
[*]      MX mail.certifiedhacker.com 162.241.216.11
[*]      CNAME www.certifiedhacker.com certifiedhacker.com
[*]      A certifiedhacker.com 162.241.216.11
[*]      TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[-] No SRV Records Found for www.certifiedhacker.com
[+] 0 Records Found
[*] Performing NSEC Zone Walk for www.certifiedhacker.com
[*] Getting SOA record for www.certifiedhacker.com
[*] Name Server 162.159.24.80 will be used
[*]      A www.certifiedhacker.com 162.241.216.11
[+] 1 records found
┌─[root@parrot]─[~]
```

Obtained record file 'A'

https://www.github.com

DNSSEC Zone Walking

Domain Name System Security Extensions (DNSSEC) zone walking is a type of DNS enumeration technique in which an attacker attempts to obtain internal records if the DNS zone is not properly configured. The enumerated zone information can assist the attacker in building a host network map.

Organizations use DNSSEC to add security features to the DNS data and provide protection against known threats to the DNS. This security feature uses digital signatures based on public-key cryptography to strengthen authentication in DNS. These digital signatures are stored in the DNS name servers along with common records such as MX, A, AAAA, and CNAME.

While DNSSEC provides Internet security, it is also susceptible to a vulnerability called zone enumeration or zone walking. By exploiting this vulnerability, attackers can obtain network information of a target domain, based on which they may launch Internet-based attacks.

To overcome the zone enumeration vulnerability, a new version of DNSSEC that uses Next Secure version 3 (NSEC3) is used. The NSEC3 record provides the same functionality as NSEC records, except that it provides cryptographically hashed record names that are designed to prevent the enumeration of record names present in the zone.

To perform zone enumeration, attackers can use various DNSSEC zone enumerators such as LDNS, DNSRecon, nsec3map, nsec3walker, and DNSwalk.

DNSSEC Zone Walking Tools

DNSSEC zone walking tools are used to enumerate the target domain's DNS record files. These tools can also perform zone enumeration on NSEC and NSEC3 record files and further use the gathered information to launch attacks such as denial-of-service (DoS) attacks and phishing attacks.

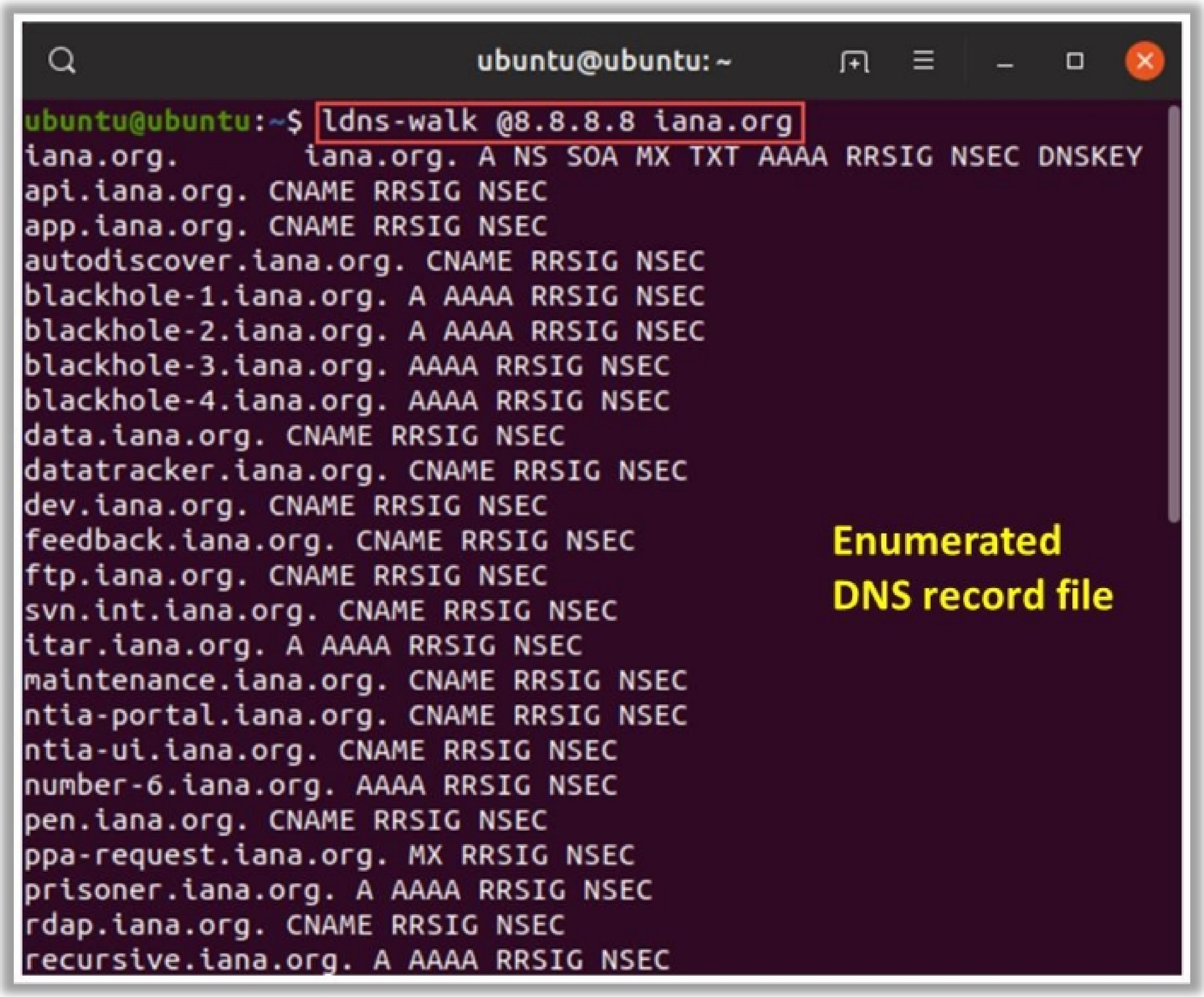
- **LDNS**

  Source: *https://www.nlnetlabs.nl*

  LDNS-walk enumerates the DNSSEC zone and obtains results on the DNS record files.

  As shown in the screenshot, attackers use the following query to enumerate a target domain `iana.org` using the DNS server `8.8.8.8` to obtain DNS record files:

  `ldns-walk @<IP of DNS Server> <Target domain>`



```
ubuntu@ubuntu:~$ ldns-walk @8.8.8.8 iana.org
iana.org.       iana.org. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY
api.iana.org. CNAME RRSIG NSEC
app.iana.org. CNAME RRSIG NSEC
autodiscover.iana.org. CNAME RRSIG NSEC
blackhole-1.iana.org. A AAAA RRSIG NSEC
blackhole-2.iana.org. A AAAA RRSIG NSEC
blackhole-3.iana.org. AAAA RRSIG NSEC
blackhole-4.iana.org. AAAA RRSIG NSEC
data.iana.org. CNAME RRSIG NSEC
datatracker.iana.org. CNAME RRSIG NSEC
dev.iana.org. CNAME RRSIG NSEC
feedback.iana.org. CNAME RRSIG NSEC
ftp.iana.org. CNAME RRSIG NSEC
svn.int.iana.org. CNAME RRSIG NSEC
itar.iana.org. A AAAA RRSIG NSEC
maintenance.iana.org. CNAME RRSIG NSEC
ntia-portal.iana.org. CNAME RRSIG NSEC
ntia-ui.iana.org. CNAME RRSIG NSEC
number-6.iana.org. AAAA RRSIG NSEC
pen.iana.org. CNAME RRSIG NSEC
ppa-request.iana.org. MX RRSIG NSEC
prisoner.iana.org. A AAAA RRSIG NSEC
rdap.iana.org. CNAME RRSIG NSEC
recursive.iana.org. A AAAA RRSIG NSEC
```

Figure 4.28: Screenshot of LDNS displaying results on the target domain

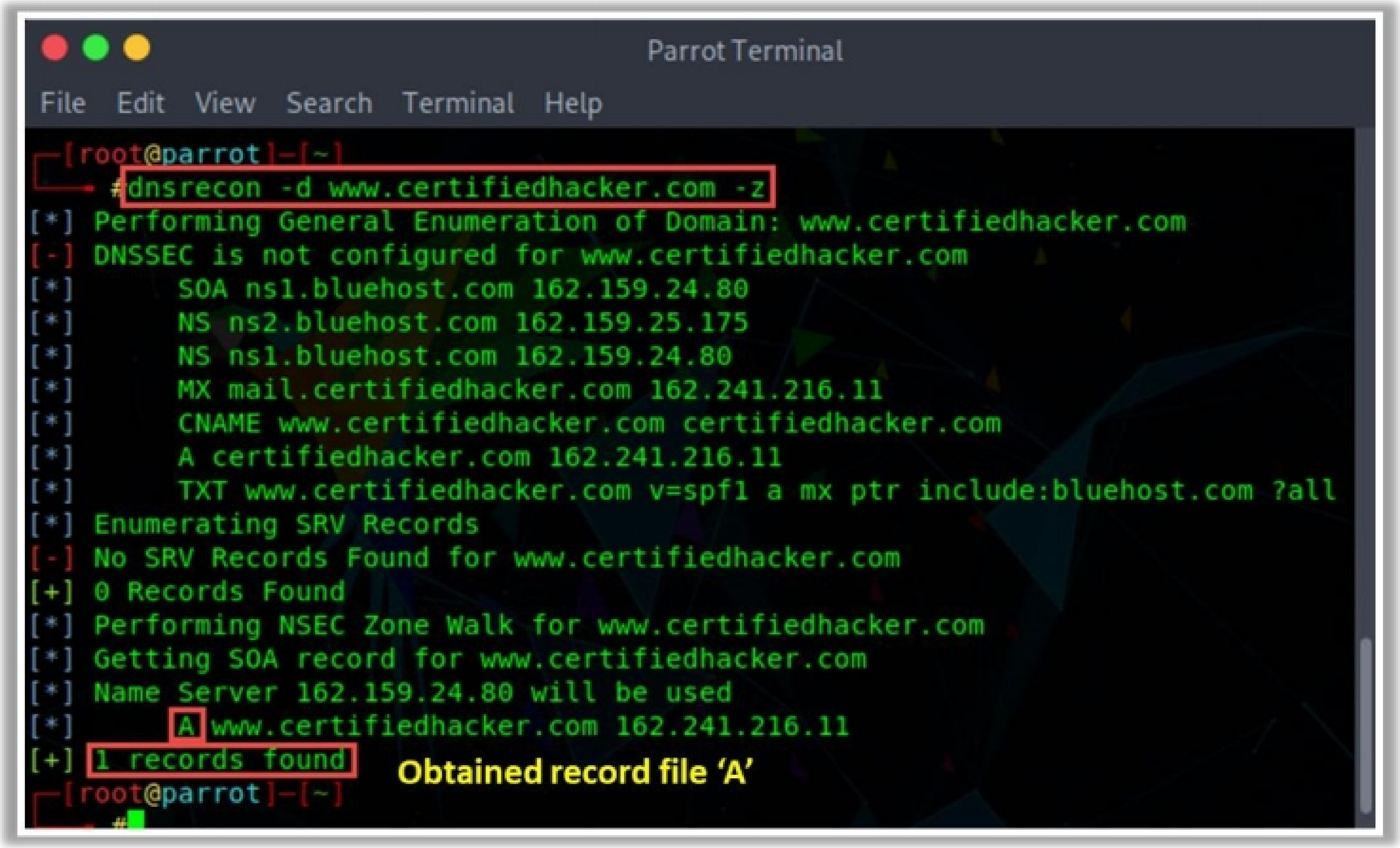
- **DNSRecon**

  Source: *https://www.github.com*

  DNSRecon is a zone enumeration tool that assists users in enumerating DNS records such as A, AAAA, and CNAME. It also performs NSEC zone enumeration to obtain DNS record files of a target domain.

  As shown in the screenshot, attackers use the following query to perform zone enumeration against a target domain **`certifiedhacker.com`**:

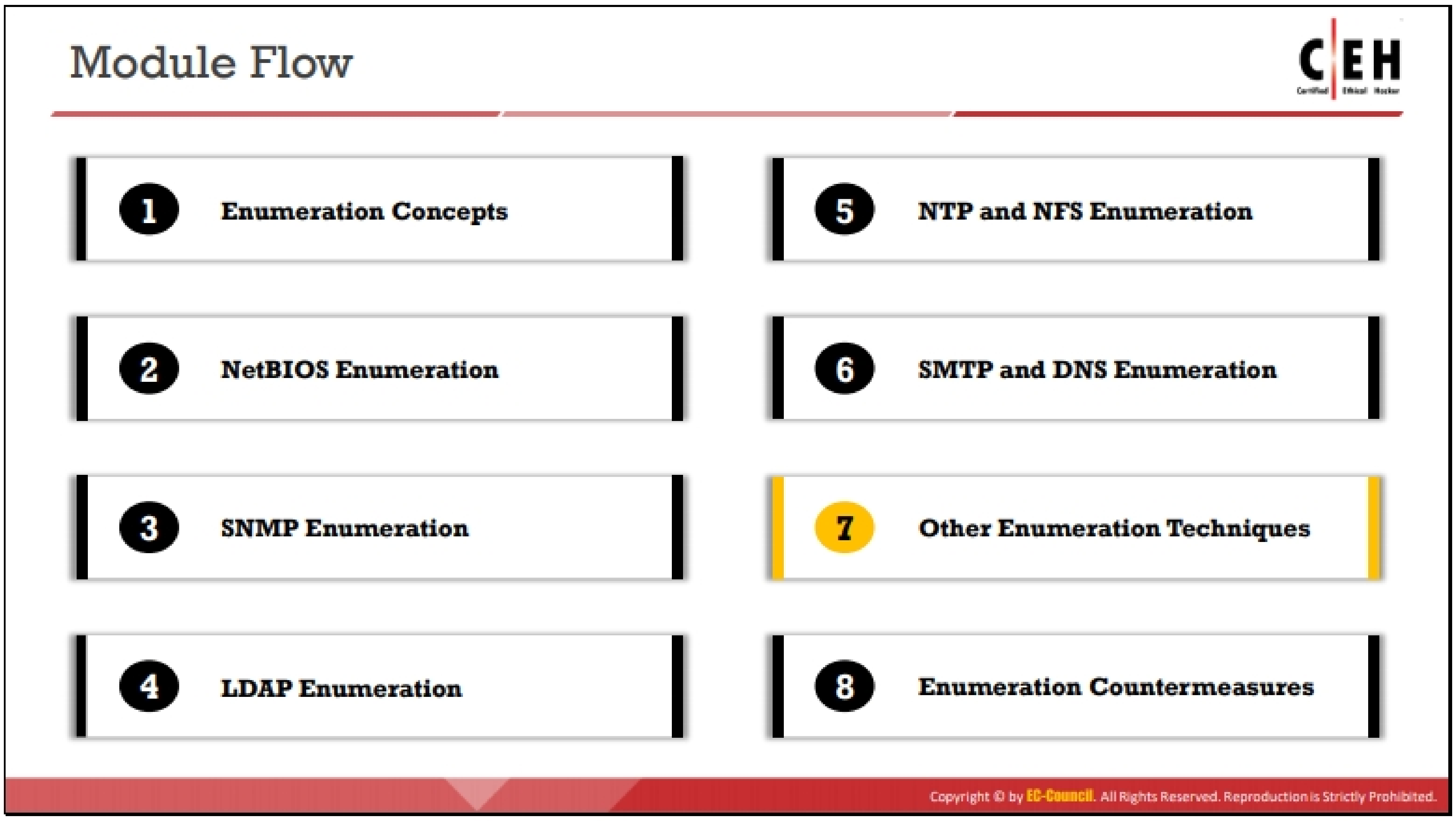
  `dnsrecon -d <target domain> -z`



```
┌─[root@parrot]─[~]
└──╼ #dnsrecon -d www.certifiedhacker.com -z
[*] Performing General Enumeration of Domain: www.certifiedhacker.com
[-] DNSSEC is not configured for www.certifiedhacker.com
[*]      SOA ns1.bluehost.com 162.159.24.80
[*]      NS ns2.bluehost.com 162.159.25.175
[*]      NS ns1.bluehost.com 162.159.24.80
[*]      MX mail.certifiedhacker.com 162.241.216.11
[*]      CNAME www.certifiedhacker.com certifiedhacker.com
[*]      A certifiedhacker.com 162.241.216.11
[*]      TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[-] No SRV Records Found for www.certifiedhacker.com
[+] 0 Records Found
[*] Performing NSEC Zone Walk for www.certifiedhacker.com
[*] Getting SOA record for www.certifiedhacker.com
[*] Name Server 162.159.24.80 will be used
[*]      A www.certifiedhacker.com 162.241.216.11
[+] 1 records found
┌─[root@parrot]─[~]
└──╼ #
```

Obtained record file 'A'

Figure 4.29: Screenshot of DNSRecon displaying results on the target domain



Module Flow

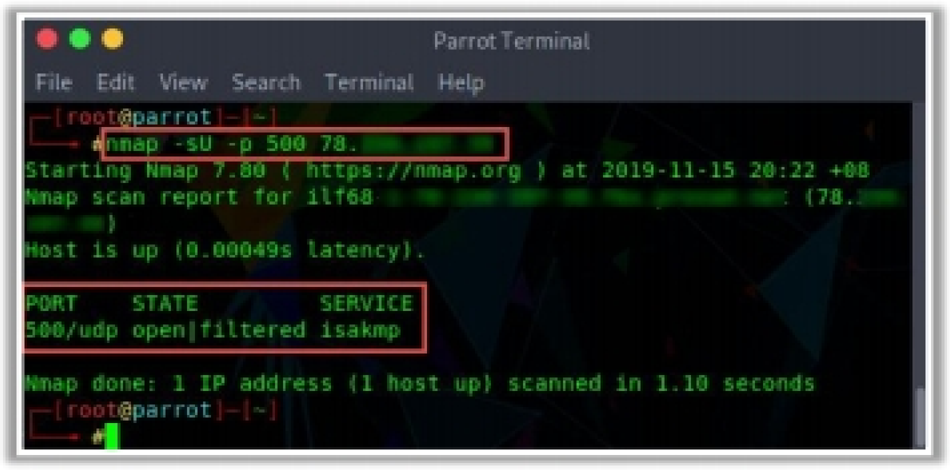
1. **Enumeration Concepts**
2. **NetBIOS Enumeration**
3. **SNMP Enumeration**
4. **LDAP Enumeration**
5. **NTP and NFS Enumeration**
6. **SMTP and DNS Enumeration**
7. **Other Enumeration Techniques**
8. **Enumeration Countermeasures**

Other Enumeration Techniques

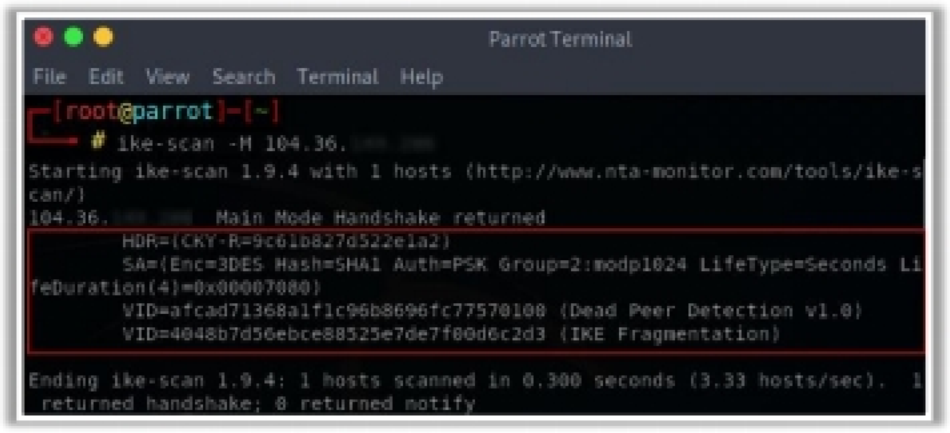
This section discusses IPsec, VoIP, RPC, Unix/Linux user, Telnet, SSH user, FTP, TFTP, SMB, IPv6, and BGP enumeration.

IPsec Enumeration

- IPsec uses Encapsulation Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE) to secure **communication between virtual private network (VPN) end points**
- Most IPsec based **VPNs use Internet Security Association and Key Management Protocol (ISAKMP)**, a part of IKE, to establish, negotiate, modify, and delete Security Associations (SA) and cryptographic keys in a VPN environment
- A simple **scanning for ISAKMP at UDP port 500** can indicate the presence of a VPN gateway
- Attackers can probe further using a tool, such as **ike-scan**, to enumerate sensitive information, including encryption and hashing algorithm, authentication type, key distribution algorithm, and SA LifeDuration



```
┌─[root@parrot]─[~]
└──╼ #nmap -sU -p 500 78.[redacted]
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 20:22 +08
Nmap scan report for ilf68 [redacted] (78.[redacted]
[redacted])
Host is up (0.00049s latency).

PORT    STATE         SERVICE
500/udp open|filtered isakmp

Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
┌─[root@parrot]─[~]
└──╼ #
```



```
┌─[root@parrot]─[~]
└──╼ # ike-scan -M 104.36.[redacted]
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-s
can/)
104.36.[redacted]   Main Mode Handshake returned
        HDR=(CKY-R=9c61b827d522e1a2)
        SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds Li
feDuration(4)=0x00007080)
        VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
        VID=4048b7d56ebce88525e7de7f00d6c2d3 (IKE Fragmentation)

Ending ike-scan 1.9.4: 1 hosts scanned in 0.300 seconds (3.33 hosts/sec).  1
 returned handshake; 0 returned notify
```

IPsec Enumeration

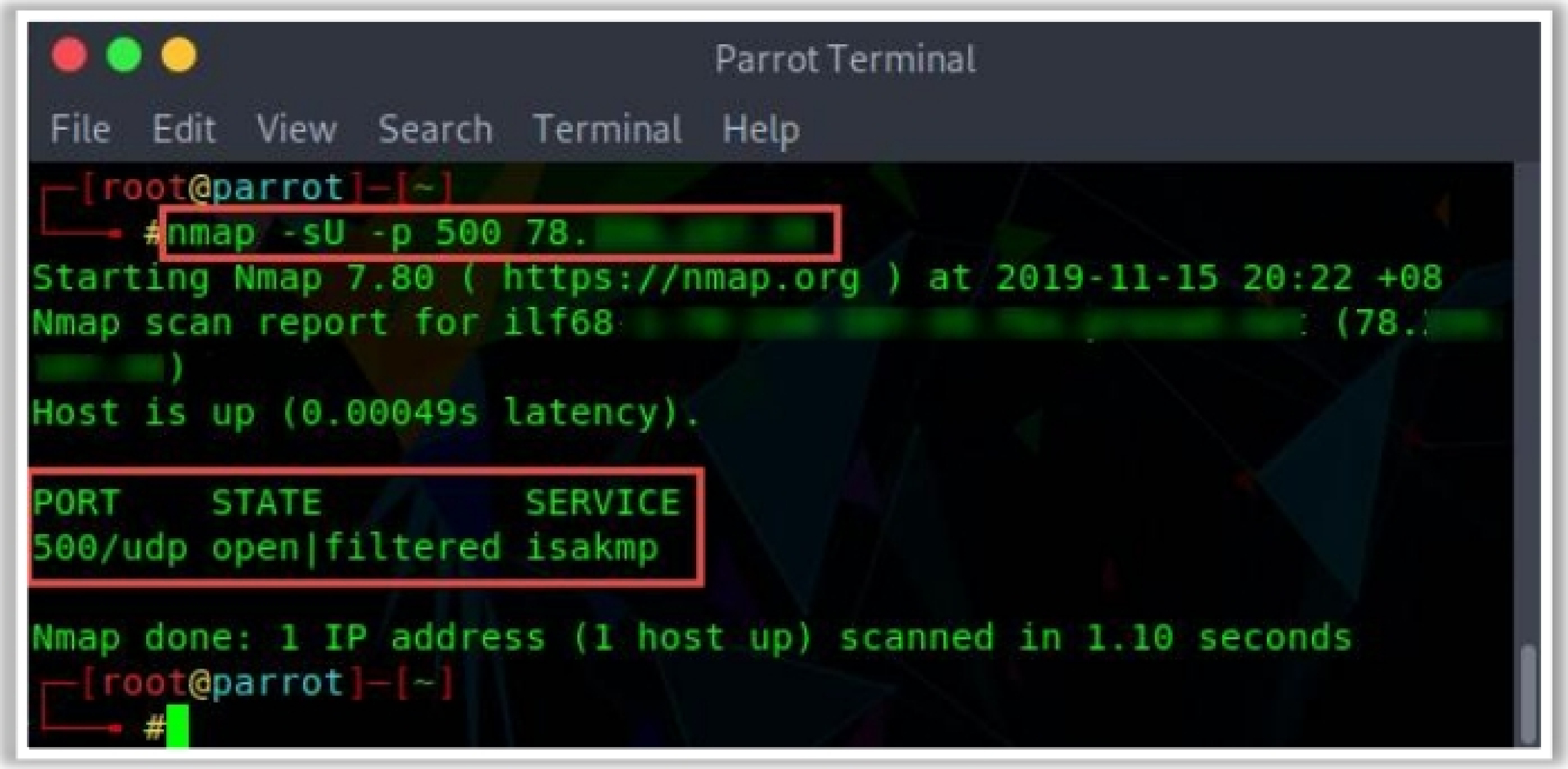
IPsec is the most commonly implemented technology for both gateway-to-gateway (LAN-to-LAN) and host-to-gateway (remote access) enterprise VPN solutions. IPsec provides data security by employing various components such as Encapsulating Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE) to secure communication between VPN endpoints.

Most IPsec-based VPNs use the Internet Security Association Key Management Protocol (ISAKMP), a part of IKE, to establish, negotiate, modify, and delete Security Associations (SA) and cryptographic keys in a VPN environment.

Attackers can perform simple direct scanning for ISAKMP at UDP port 500 with tools such as Nmap to acquire information related to the presence of a VPN gateway.

The following command can be used to perform an Nmap scan for checking the status of ISAKMP over port 500:

```
# nmap –sU –p 500 <target IP address>
```



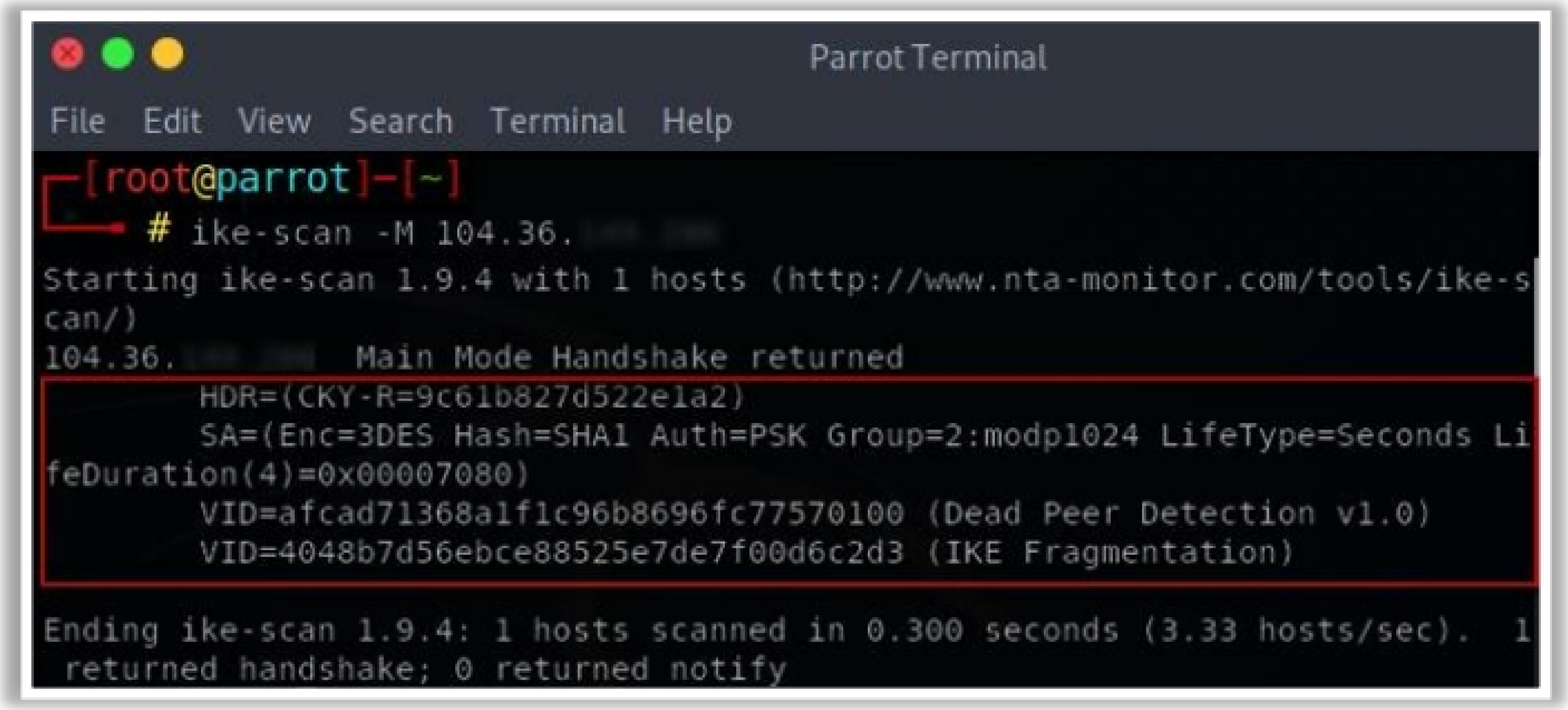
```
┌─[root@parrot]─[~]
└──╼ #nmap -sU -p 500 78.[redacted]
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 20:22 +08
Nmap scan report for ilf68[redacted] (78.[redacted])
Host is up (0.00049s latency).

PORT    STATE         SERVICE
500/udp open|filtered isakmp

Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
┌─[root@parrot]─[~]
└──╼ #
```

Figure 4.30: Screenshot displaying an Nmap scan over port 500 for ISAKMP

Attackers can probe further using fingerprinting tools such as ike-scan to enumerate sensitive information, including the encryption and hashing algorithm, authentication type, key distribution algorithm, and SA LifeDuration. In this type of scan, specially crafted IKE packets with an ISAKMP header are sent to the target gateway, and the responses are recorded.

The following command is used for initial IPsec VPN discovery with ike-scan tool:

```
# ike-scan –M <target gateway IP address>
```



```
┌─[root@parrot]─[~]
└──╼ # ike-scan -M 104.36.[redacted]
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-s
can/)
104.36.[redacted]  Main Mode Handshake returned
        HDR=(CKY-R=9c61b827d522e1a2)
        SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds Li
feDuration(4)=0x00007080)
        VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
        VID=4048b7d56ebce88525e7de7f00d6c2d3 (IKE Fragmentation)

Ending ike-scan 1.9.4: 1 hosts scanned in 0.300 seconds (3.33 hosts/sec).  1
 returned handshake; 0 returned notify
```

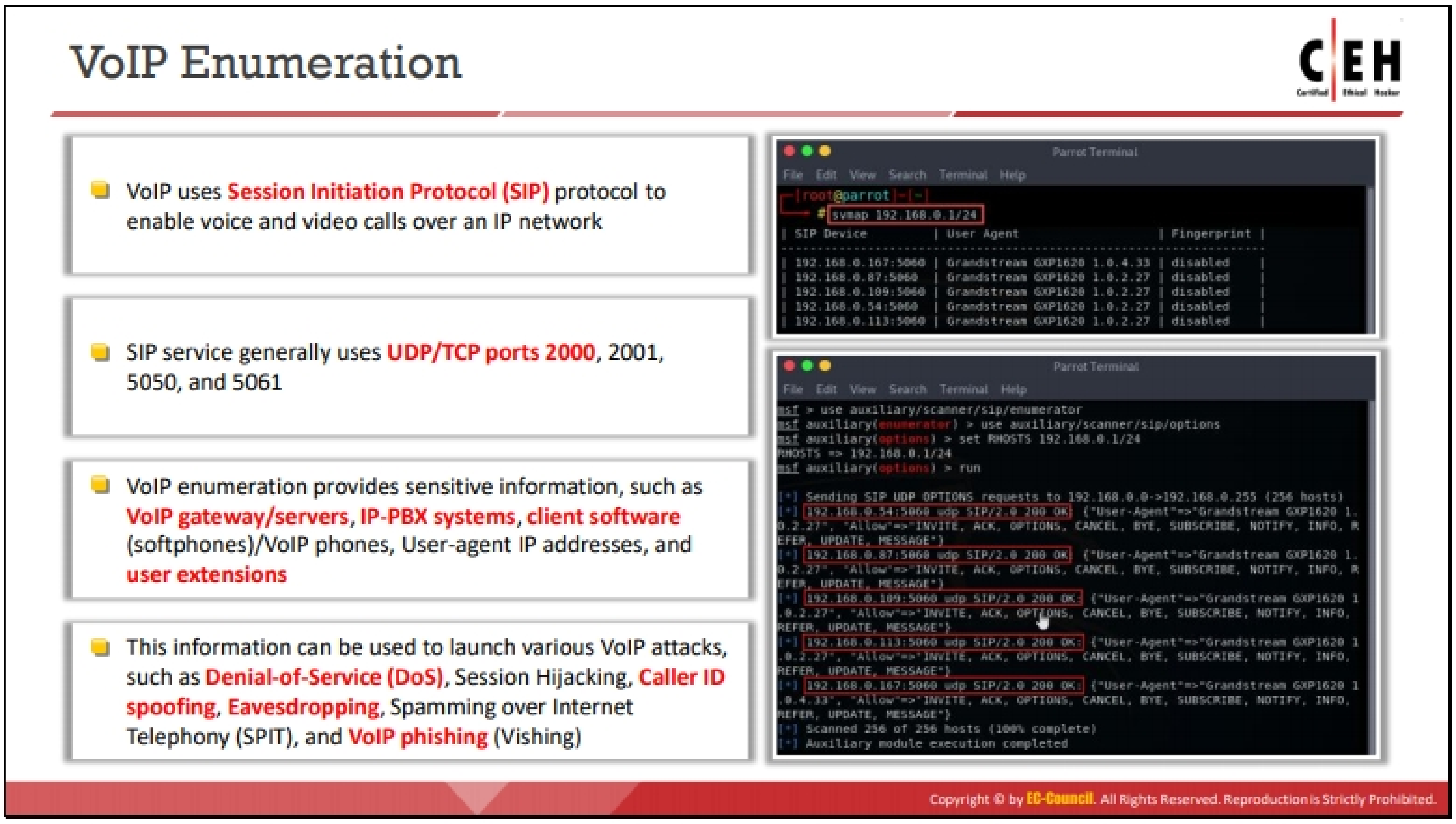
Figure 4.31: Screenshot displaying ike-scan enumeration

ike-scan

Source: *https://github.com*

ike-scan discovers IKE hosts and can fingerprint them using the retransmission backoff pattern. ike-scan can perform the following functions.

- **Discovery**: The hosts running IKE in a given IP range can be determined by displaying the hosts that respond to the IKE requests sent by ike-scan.
- **Fingerprinting**: The IKE implementation used by the hosts can be determined, and in some cases, the version of the software they are running can be determined. This is done in two ways: UDP backoff fingerprinting, which involves recording the times of arrival of the IKE response packets from the target hosts and comparing the observed retransmission backoff pattern against known patterns, and Vendor ID fingerprinting, which compares Vendor ID payloads from the VPN servers against known Vendor ID patterns.
- **Transform enumeration**: The transform attributes supported by the VPN server for IKE phase 1 (e.g., encryption algorithm and hash algorithm) can be determined.
- **User enumeration**: For some VPN systems, valid VPN usernames can be discovered.
- **Pre-shared key cracking**: Offline dictionary or brute-force password cracking can be performed for IKE Aggressive Mode with pre-shared key authentication. This uses ike-scan to obtain the hash and other parameters as well as psk-crack, which is a part of the ike-scan package, to perform the cracking.



VoIP Enumeration

- VoIP uses **Session Initiation Protocol (SIP)** protocol to enable voice and video calls over an IP network
- SIP service generally uses **UDP/TCP ports 2000**, 2001, 5050, and 5061
- VoIP enumeration provides sensitive information, such as **VoIP gateway/servers**, **IP-PBX systems**, **client software** (softphones)/VoIP phones, User-agent IP addresses, and **user extensions**
- This information can be used to launch various VoIP attacks, such as **Denial-of-Service (DoS)**, Session Hijacking, **Caller ID spoofing**, **Eavesdropping**, Spamming over Internet Telephony (SPIT), and **VoIP phishing** (Vishing)

```
┌─[root@parrot]─[~]
└──╼ #svmap 192.168.0.1/24
| SIP Device         | User Agent                    | Fingerprint |
----------------------------------------------------------------------
| 192.168.0.167:5060 | Grandstream GXP1620 1.0.4.33 | disabled    |
| 192.168.0.87:5060  | Grandstream GXP1620 1.0.2.27 | disabled    |
| 192.168.0.109:5060 | Grandstream GXP1620 1.0.2.27 | disabled    |
| 192.168.0.54:5060  | Grandstream GXP1620 1.0.2.27 | disabled    |
| 192.168.0.113:5060 | Grandstream GXP1620 1.0.2.27 | disabled    |
```

```
msf > use auxiliary/scanner/sip/enumerator
msf auxiliary(enumerator) > use auxiliary/scanner/sip/options
msf auxiliary(options) > set RHOSTS 192.168.0.1/24
RHOSTS => 192.168.0.1/24
msf auxiliary(options) > run

[*] Sending SIP UDP OPTIONS requests to 192.168.0.0->192.168.0.255 (256 hosts)
[*] 192.168.0.54:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1.
0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, R
EFER, UPDATE, MESSAGE"}
[*] 192.168.0.87:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1.
0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, R
EFER, UPDATE, MESSAGE"}
[*] 192.168.0.109:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1
.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] 192.168.0.113:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1
.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] 192.168.0.167:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1
.0.4.33", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

VoIP Enumeration

VoIP is an advanced technology that has replaced the conventional public switched telephone network (PSTN) in both corporate and home environments. VoIP uses internet infrastructure to establish connections for voice calls; data are also transmitted on the same network. However, VoIP is vulnerable to TCP/IP attack vectors. Session Initiation Protocol (SIP) is one of the protocols used by VoIP for performing voice calls, video calls, etc. over an IP network. This SIP service generally uses UDP/TCP ports 2000, 2001, 5050, and 5061.

Attackers use Svmap and Metasploit tools to perform VoIP enumeration. Through VoIP enumeration, attackers can gather sensitive information such as VoIP gateway/servers, IP-private branch exchange (PBX) systems, and User-Agent IP addresses and user extensions of client software (softphones) or VoIP phones. This information can be used to launch various VoIP attacks such as DoS attacks, session hijacking, caller ID spoofing, eavesdropping, spam over Internet telephony (SPIT), and VoIP phishing (Vishing).

- **Svmap**

  Source: *https://github.com*

  Svmap is an open-source scanner that identifies SIP devices and PBX servers on a target network. It can be helpful for system administrators when used as a network inventory tool.

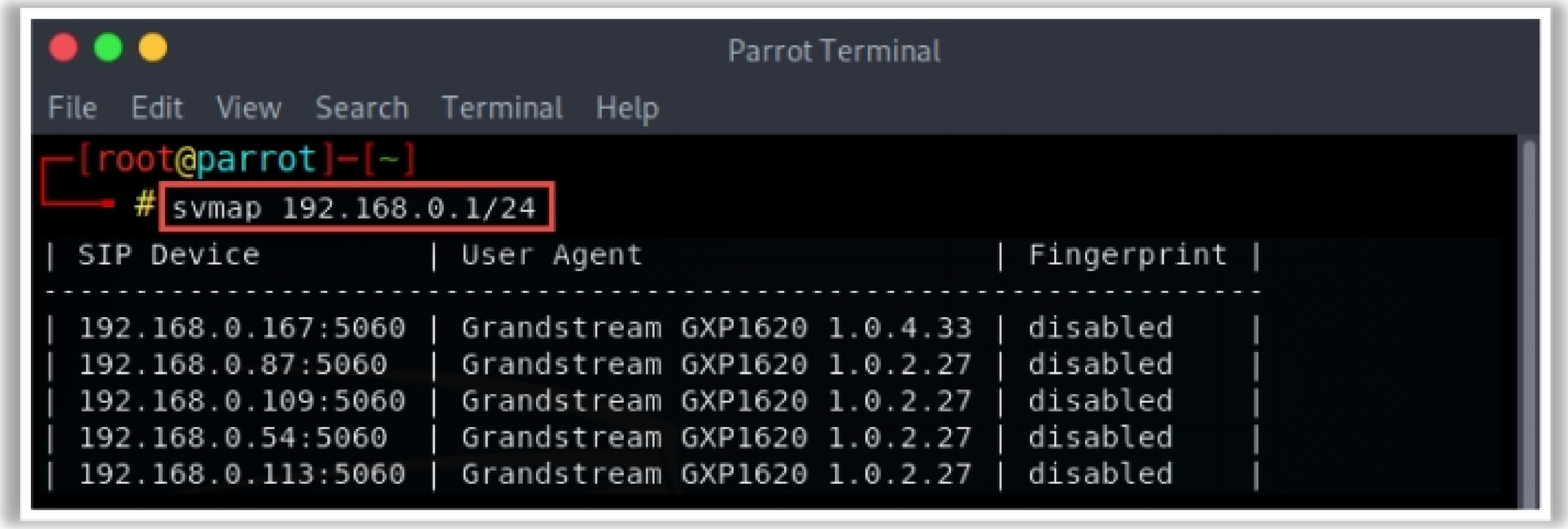
  Attackers use Svmap to perform the following:

  - Identify SIP devices and PBX servers on default and non-default ports
  - Scan large ranges of networks

- Scan one host on different ports for an SIP service on that host or multiple hosts on multiple ports
- Ring all the phones on a network simultaneously using the INVITE method

Below screenshot shows an example for the enumeration of SIP device details using the Svmap tool through the following command:

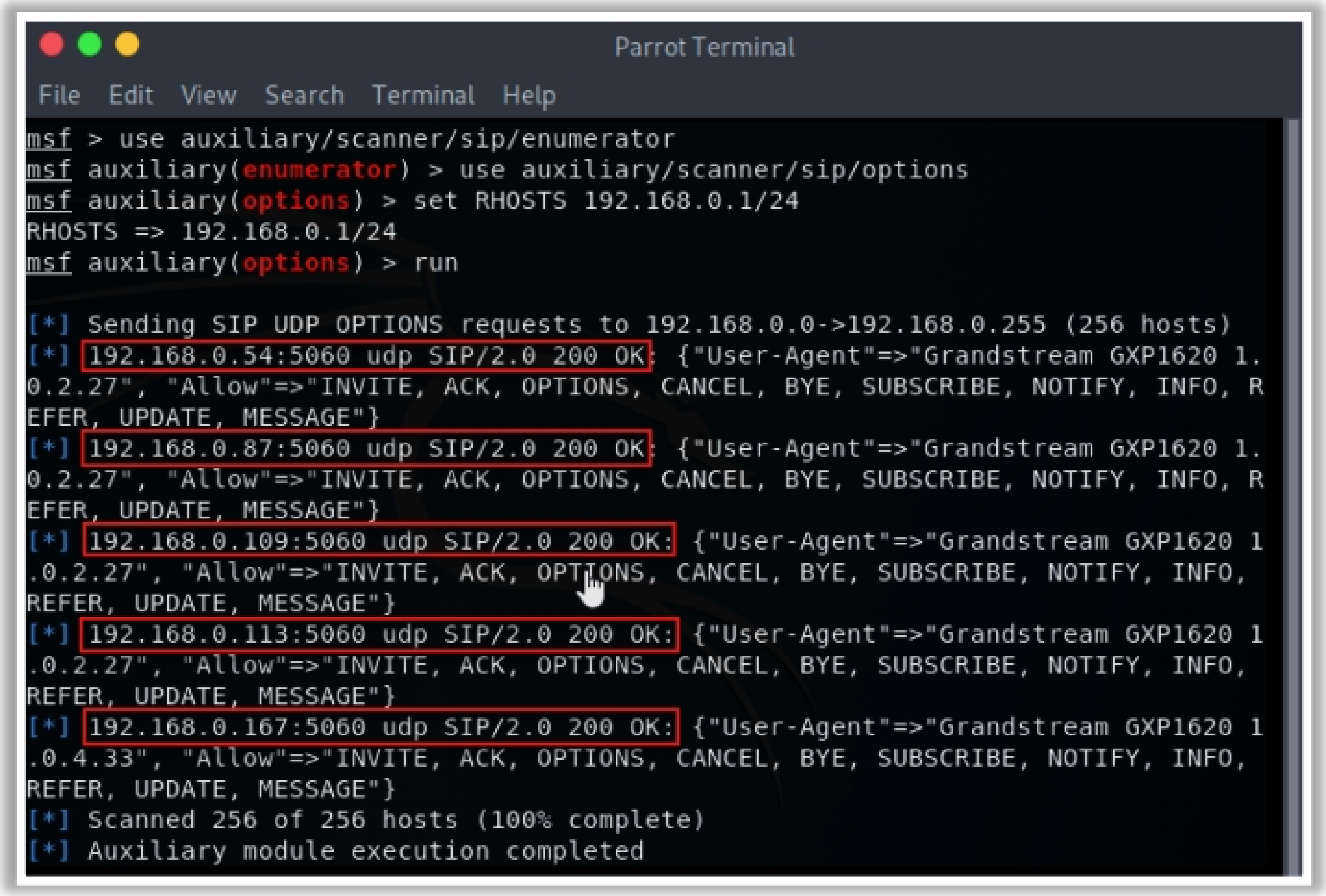
`# svmap <target network range>`



```
┌─[root@parrot]─[~]
└──╼ #svmap 192.168.0.1/24
| SIP Device         | User Agent                   | Fingerprint |
-------------------------------------------------------------------
| 192.168.0.167:5060 | Grandstream GXP1620 1.0.4.33 | disabled    |
| 192.168.0.87:5060  | Grandstream GXP1620 1.0.2.27 | disabled    |
| 192.168.0.109:5060 | Grandstream GXP1620 1.0.2.27 | disabled    |
| 192.168.0.54:5060  | Grandstream GXP1620 1.0.2.27 | disabled    |
| 192.168.0.113:5060 | Grandstream GXP1620 1.0.2.27 | disabled    |
```

Figure 4.32: Screenshot displaying Svmap scan for enumerating SIP details

Attackers use Metasploit's SIP Username Enumerator to scan numeric usernames/extensions of VoIP phones. Below screenshot shows an example for enumerating SIP using Metasploit.

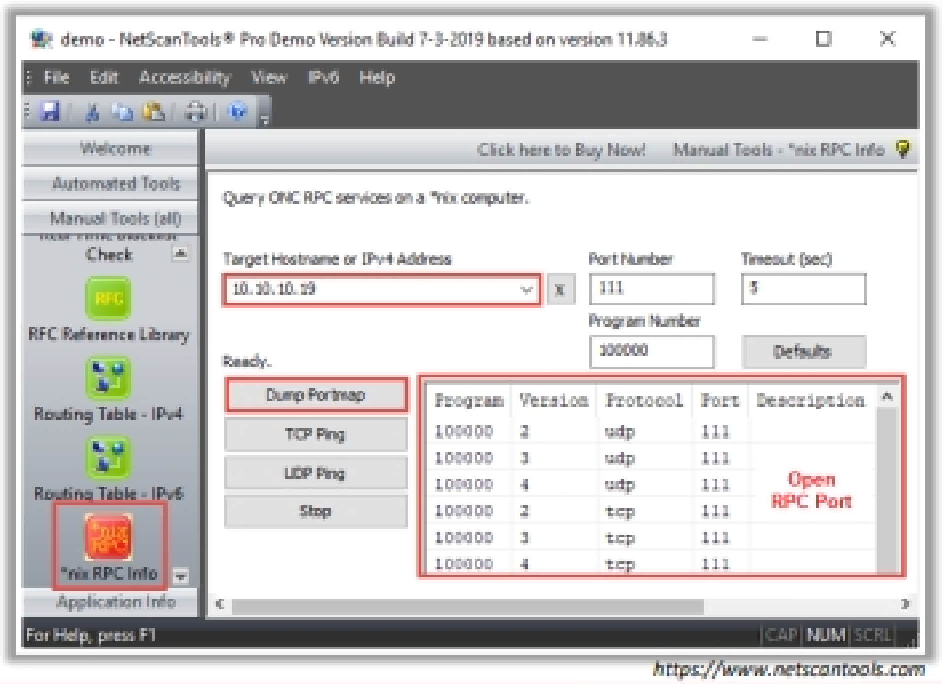


```
msf > use auxiliary/scanner/sip/enumerator
msf auxiliary(enumerator) > use auxiliary/scanner/sip/options
msf auxiliary(options) > set RHOSTS 192.168.0.1/24
RHOSTS => 192.168.0.1/24
msf auxiliary(options) > run

[*] Sending SIP UDP OPTIONS requests to 192.168.0.0->192.168.0.255 (256 hosts)
[*] 192.168.0.54:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1.
0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, R
EFER, UPDATE, MESSAGE"}
[*] 192.168.0.87:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1.
0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, R
EFER, UPDATE, MESSAGE"}
[*] 192.168.0.109:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1
.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] 192.168.0.113:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1
.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] 192.168.0.167:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1
.0.4.33", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 4.33: Screenshot displaying Metasploit exploit for SIP enumeration

RPC Enumeration

- Remote Procedure Call (RPC) allows clients and servers to communicate in **distributed client/server programs**
- Enumerating RPC endpoints enables attackers to **identify any vulnerable services** on these service ports


demo - NetScanTools® Pro Demo Version Build 7-3-2019 based on version 11.86.3
File
Edit
Accessibility
View
IPv6
Help
Welcome
Automated Tools
Manual Tools (all)
Check
RFC Reference Library
Routing Table - IPv4
Routing Table - IPv6
*nix RPC Info
Application Info
Click here to Buy Now!
Manual Tools - *nix RPC Info
Dump Portmap
TCP Ping
UDP Ping
Stop
Defaults
For Help, press F1
CAP
NUM
SCRL

Query ONC RPC services on a *nix computer.

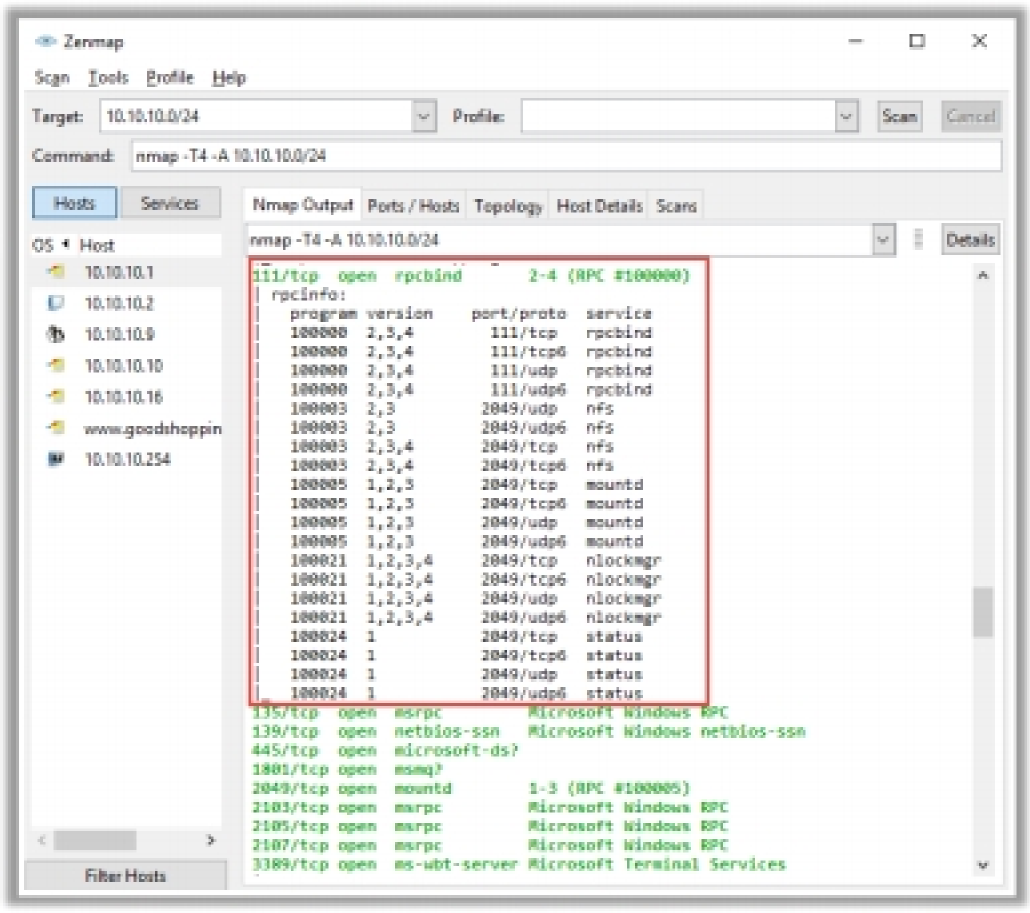
Target Hostname or IPv4 Address: 10.10.10.19
Port Number: 111
Timeout (sec): 5
Program Number: 100000

Ready.

Program	Version	Protocol	Port	Description
100000	2	udp	111	
100000	3	udp	111	
100000	4	udp	111	
100000	2	tcp	111	
100000	3	tcp	111	
100000	4	tcp	111	

Open RPC Port

https://www.netscantools.com


Zenmap
Scan
Tools
Profile
Help
Profile:
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
OS
Host
10.10.10.1
10.10.10.2
10.10.10.9
10.10.10.10
10.10.10.16
www.goodshoppin
10.10.10.254
Filter Hosts

Target: 10.10.10.0/24
Command: nmap -T4 -A 10.10.10.0/24

```
111/tcp  open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1801/tcp open  msmq?
2049/tcp open  mountd        1-3 (RPC #100005)
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

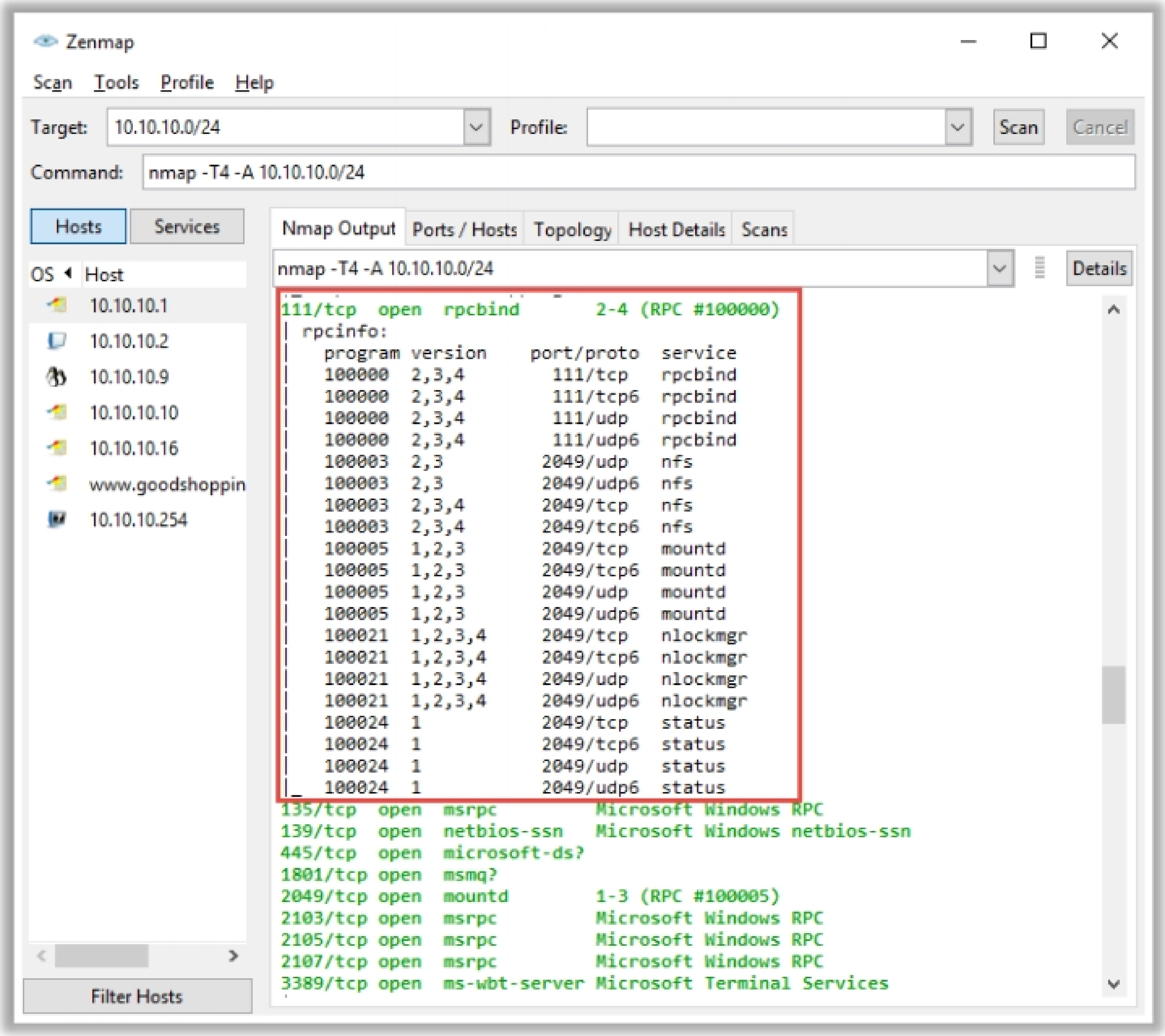
RPC Enumeration

The remote procedure call (RPC) is a technology used for creating distributed client/server programs. RPC allows clients and servers to communicate in distributed client/server programs. It is an inter-process communication mechanism, which enables data exchange between different processes. In general, RPC consists of components such as a client, a server, an endpoint, an endpoint mapper, a client stub, and a server stub, along with various dependencies.

The portmapper service listens on TCP and UDP port 111 to detect the endpoints and present clients, along with details of listening RPC services. Enumerating RPC endpoints enables attackers to identify any vulnerable services on these service ports. In networks protected by firewalls and other security establishments, this portmapper is often filtered. Therefore, attackers scan wide port ranges to identify RPC services that are open to direct attack.

Attackers use the following Nmap scan commands to identify the RPC service running on the network:

```
# nmap -sR <target IP/network>
# nmap -T4 -A <target IP/network>
```


Zenmap
Scan
Tools
Profile
Help
Target:
Profile:
Scan
Cancel
Command:
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
OS
Host
10.10.10.1
10.10.10.2
10.10.10.9
10.10.10.10
10.10.10.16
www.goodshoppin
10.10.10.254
Filter Hosts

Target: 10.10.10.0/24

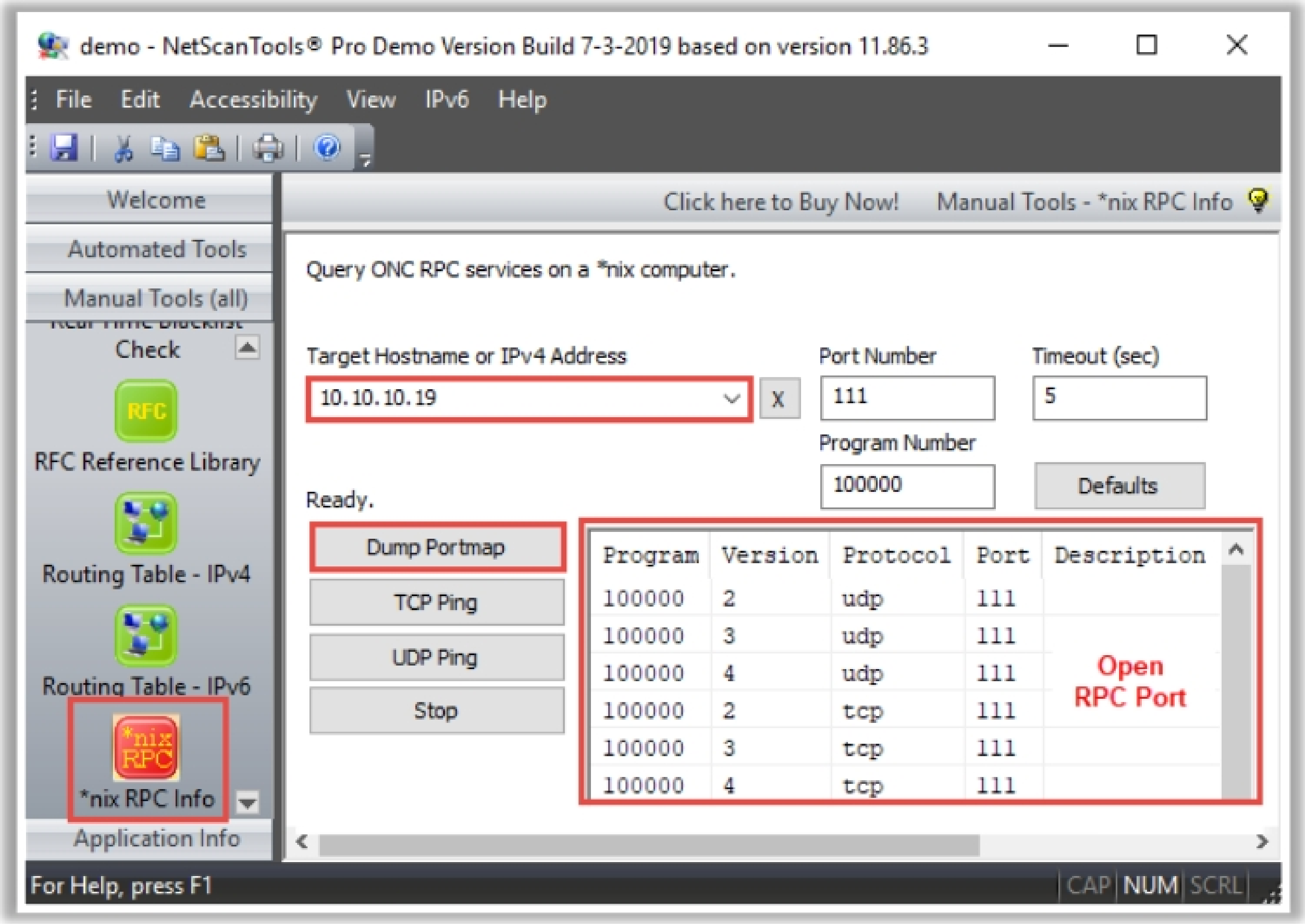
Command: nmap -T4 -A 10.10.10.0/24

```
nmap -T4 -A 10.10.10.0/24
```

```
111/tcp  open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1801/tcp open  msmq?
2049/tcp open  mountd        1-3 (RPC #100005)
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

Figure 4.34: Screenshot displaying an Nmap scan result for RPC enumeration

Additionally, attackers use tools such as NetScanTools Pro to capture the RPC information of the target network. The NetScanTools Pro RPC Info tool helps attackers detect and access the portmapper daemon/service that typically runs on port 111 of Unix or Linux machines.


demo - NetScanTools® Pro Demo Version Build 7-3-2019 based on version 11.86.3
File
Edit
Accessibility
View
IPv6
Help
Welcome
Automated Tools
Manual Tools (all)
Check
RFC
RFC Reference Library
Routing Table - IPv4
Routing Table - IPv6
*nix RPC
*nix RPC Info
Application Info
Click here to Buy Now!
Manual Tools - *nix RPC Info
Dump Portmap
TCP Ping
UDP Ping
Stop
Defaults
X
Open RPC Port
For Help, press F1
CAP
NUM
SCRL

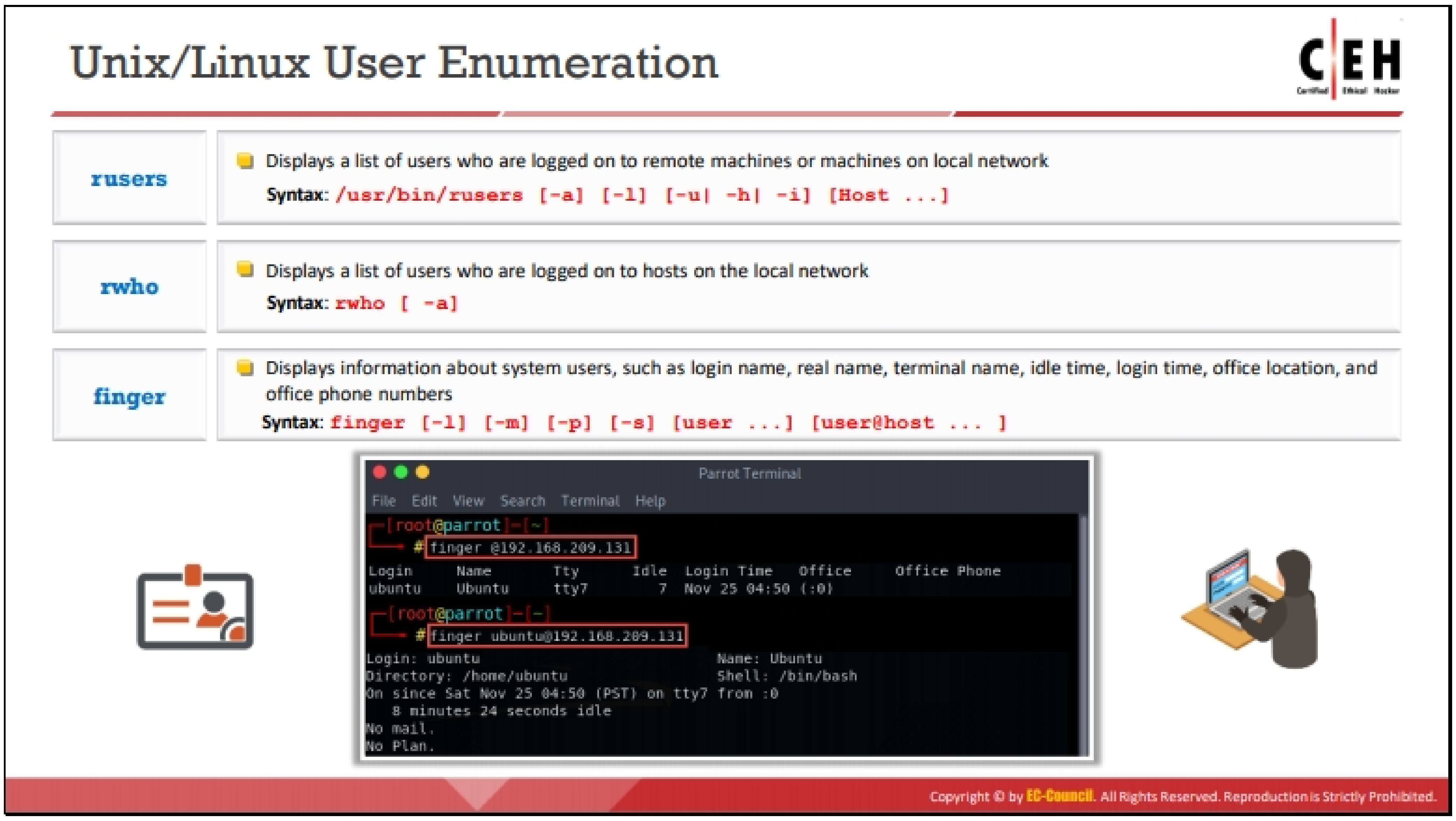
Query ONC RPC services on a *nix computer.

Target Hostname or IPv4 Address: 10.10.10.19
Port Number: 111
Timeout (sec): 5
Program Number: 100000

Ready.

Program	Version	Protocol	Port	Description
100000	2	udp	111	
100000	3	udp	111	
100000	4	udp	111	
100000	2	tcp	111	
100000	3	tcp	111	
100000	4	tcp	111	

Figure 4.35: Screenshot displaying NetScanTools Pro tool for RPC enumeration



Unix/Linux User Enumeration

rusers	Displays a list of users who are logged on to remote machines or machines on local network **Syntax**: `/usr/bin/rusers [-a] [-l] [-u| -h| -i] [Host ...]`
rwho	Displays a list of users who are logged on to hosts on the local network **Syntax**: `rwho [ -a]`
finger	Displays information about system users, such as login name, real name, terminal name, idle time, login time, office location, and office phone numbers **Syntax**: `finger [-l] [-m] [-p] [-s] [user ...] [user@host ... ]`

```
┌─[root@parrot]─[~]
└──╼ #finger @192.168.209.131
Login     Name       Tty      Idle  Login Time   Office     Office Phone
ubuntu    Ubuntu     tty7        7  Nov 25 04:50 (:0)
┌─[root@parrot]─[~]
└──╼ #finger ubuntu@192.168.209.131
Login: ubuntu                           Name: Ubuntu
Directory: /home/ubuntu                 Shell: /bin/bash
On since Sat Nov 25 04:50 (PST) on tty7 from :0
   8 minutes 24 seconds idle
No mail.
No Plan.
```

Unix/Linux User Enumeration

One of the important steps for enumeration is to perform Unix/Linux user enumeration. Unix/Linux user enumeration provides a list of users along with details such as the username, host name, and start date and time of each session.

The following command-line utilities can be used to perform Unix/Linux user enumeration.

- **rusers**

  rusers displays a list of users who are logged in to remote machines or machines on the local network. It displays an output similar to the who command, but for the hosts/systems on the local network. Its syntax is as follows:

  `/usr/bin/rusers [-a] [-l] [-u| -h| -i] [Host ...]`

  The options are as follows.

  - **-a**: Gives a report for a machine even if no users are logged in
  - **-h**: Sorts alphabetically by host name
  - **-l**: Gives a longer listing similar to the who command
  - **-u**: Sorts by the number of users
  - **-i**: Sorts by idle time

- **rwho**

  rwho displays a list of users who are logged in to hosts on the local network. Its output is similar to that of the who command and contains information about the username, host name, and start date and time of each session for all machines on the local network running the rwho daemon. Its syntax is as follows:

```
rwho [ -a]
```

It has the following option.

- **-a**: Includes all users; without this flag, users whose sessions are idle for an hour or more are not included in the report

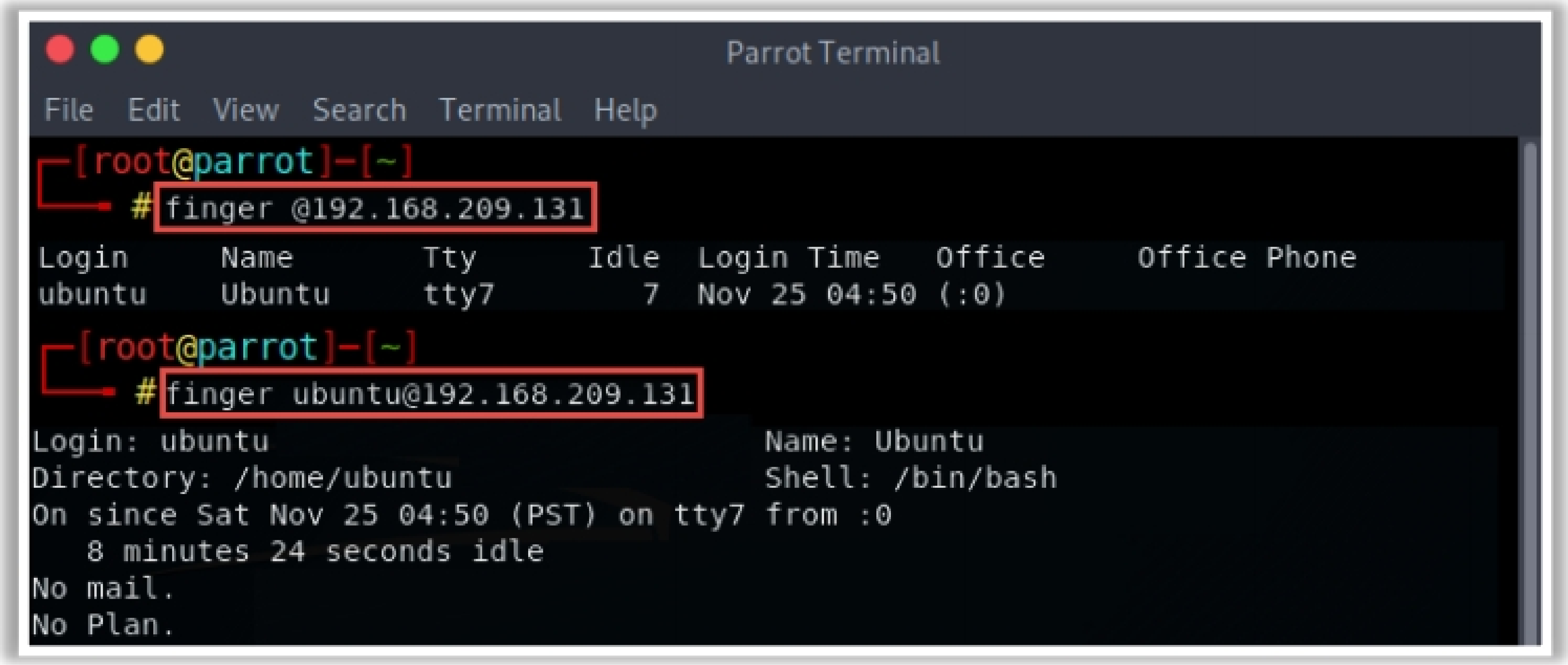
- **finger**

  finger displays information about system users such as the user's login name, real name, terminal name, idle time, login time, office location, and office phone numbers. Its syntax is as follows:

  ```
  finger [-l] [-m] [-p] [-s] [user ...] [user@host ...]
  ```

  The options are as follows.

  - **-s**: Displays the user's login name, real name, terminal name, idle time, login time, office location, and office phone number
  - **-l**: Produces a multi-line format displaying all of the information described for the -s option as well as the user's home directory, home phone number, login shell, mail status, and the contents of the files ".plan," ".project," ".pgpkey," and ".forward" from the user's home directory
  - **-p**: Prevents the -l option of finger from displaying the contents of the ".plan," ".project," and ".pgpkey" files.
  - **-m**: Prevents the matching of usernames.



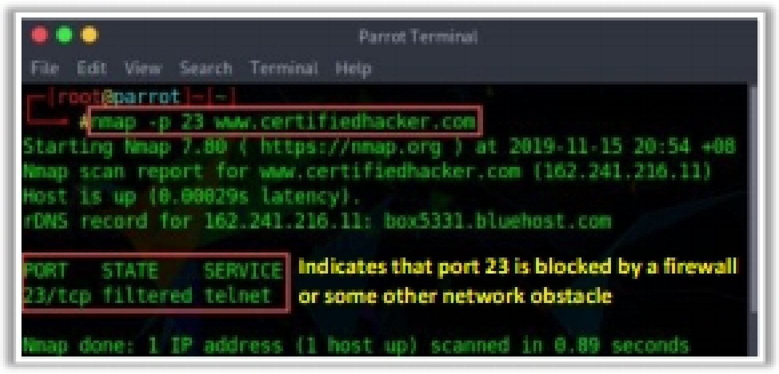
```
┌─[root@parrot]─[~]
└──╼ #finger @192.168.209.131
Login     Name       Tty      Idle  Login Time   Office     Office Phone
ubuntu    Ubuntu     tty7        7  Nov 25 04:50 (:0)
┌─[root@parrot]─[~]
└──╼ #finger ubuntu@192.168.209.131
Login: ubuntu                           Name: Ubuntu
Directory: /home/ubuntu                 Shell: /bin/bash
On since Sat Nov 25 04:50 (PST) on tty7 from :0
   8 minutes 24 seconds idle
No mail.
No Plan.
```

Figure 4.36: Screenshot displaying the execution of the finger command for user enumeration

Telnet and SMB Enumeration

Telnet Enumeration

- If the Telnet port is found open, attackers can **access shared information**, including the hardware and software information of the target
- Telnet enumeration enables attackers to **exploit identified vulnerabilities** and perform brute-force attacks to gain unauthorized access to the target and launch further attacks

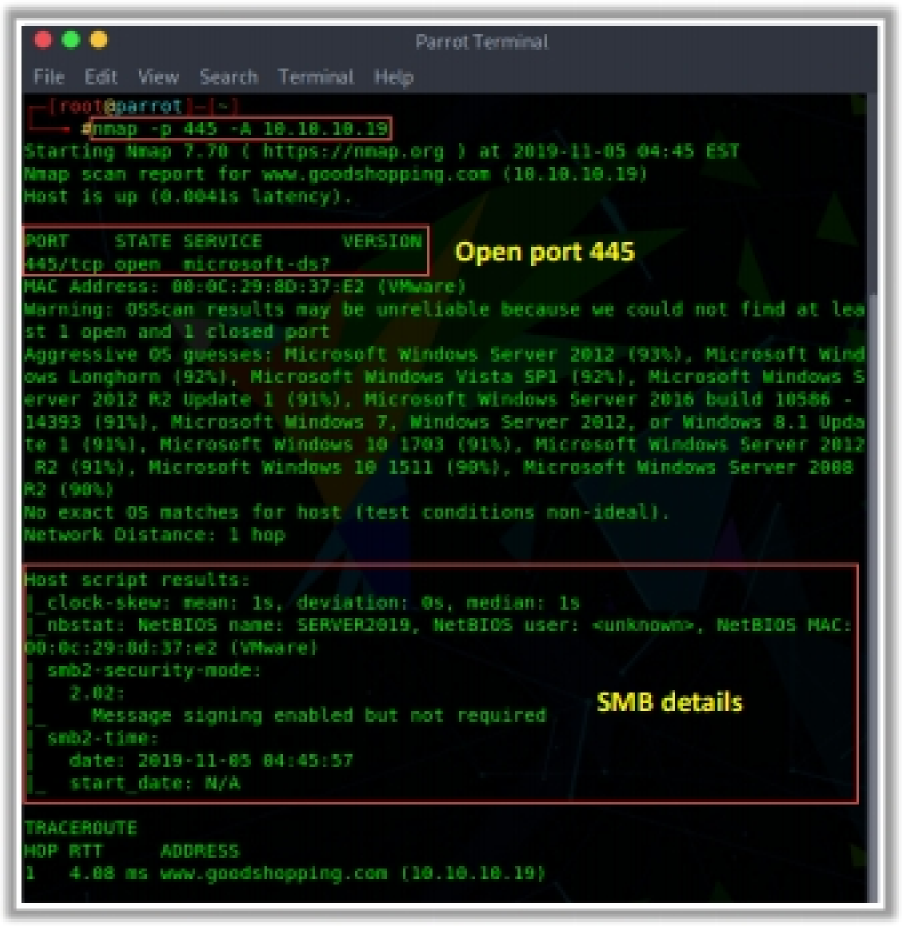


```
┌─[root@parrot]─[~]
└──╼ #nmap -p 23 www.certifiedhacker.com
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 20:54 +08
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.00029s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT   STATE    SERVICE
23/tcp filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
```

Indicates that port 23 is blocked by a firewall or some other network obstacle

SMB Enumeration

- Attackers use SMB enumeration tools, such as **Nmap**, **SMBMap**, **enum4linux**, and **nullinux**, to perform a directed scan on the SMB service running on port 445
- SMB enumeration helps attackers to perform **OS banner grabbing** on the target



```
┌─[root@parrot]─[~]
└──╼ #nmap -p 445 -A 10.10.10.19
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-05 04:45 EST
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.0041s latency).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?
MAC Address: 00:0C:29:8D:37:E2 (VMware)
Warning: OSScan results may be unreliable because we could not find at lea
st 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 (93%), Microsoft Wind
ows Longhorn (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows S
erver 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 -
14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Upda
te 1 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows Server 2012
 R2 (91%), Microsoft Windows 10 1511 (90%), Microsoft Windows Server 2008
R2 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
|_nbstat: NetBIOS name: SERVER2019, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:8d:37:e2 (VMware)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-11-05 04:45:57
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   4.08 ms www.goodshopping.com (10.10.10.19)
```

Open port 445

SMB details

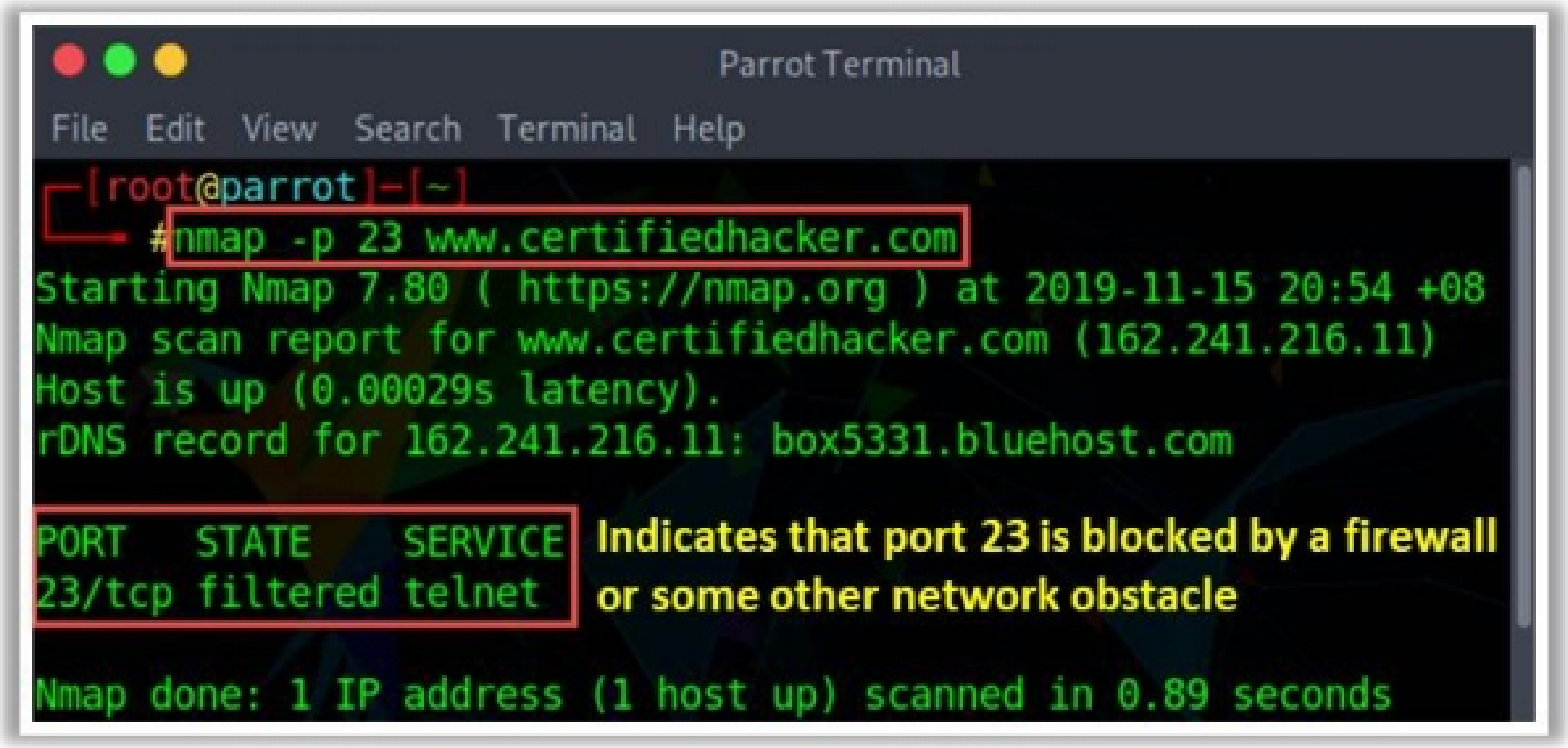
Telnet Enumeration

Telnet is a network terminal protocol that allows users to access remote computers or servers over the Internet. This protocol provides two-way interactive communication for computers on LANs and the Internet. Depending on the privileges assigned to the users, they can use Telnet to log in to the remote system to access specific files, services, data, etc.

Attackers perform port scanning to gather information regarding open ports and services on the target server. If the Telnet port is found to be open, attackers can learn about the information being shared, including hardware and software information of the target. By using this information, attackers can exploit their specific vulnerabilities and perform a brute-force attack to gain unauthorized access to the target system. Attackers can use the Nmap tool to perform simple direct scanning for Telnet port 23.

As shown in the screenshot, the following Nmap command is used by attackers to enumerate the Telnet service running on the target system:

```
# nmap -p 23 <target domain>
```



```
┌─[root@parrot]─[~]
└──╼ #nmap -p 23 www.certifiedhacker.com
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 20:54 +08
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.00029s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT   STATE    SERVICE
23/tcp filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
```

Indicates that port 23 is blocked by a firewall or some other network obstacle

Figure 4.37: Screenshot of Nmap displaying a Telnet enumeration result

Attackers can further use the following script to enumerate information from remote Microsoft Telnet services with New Technology LAN Manager (NTLM) authentication enabled:

```
# nmap -p 23 --script telnet-ntlm-info <target IP>
```

Once the information about the target server is obtained, the attackers can use the following script to perform a brute-force attack against the Telnet server:

```
# nmap -p 23 –script telnet-brute.nse –script-args
userdb=/root/Desktop/user.txt,passdb=/root/Desktop/pass.txt <target
IP>
```

SMB Enumeration

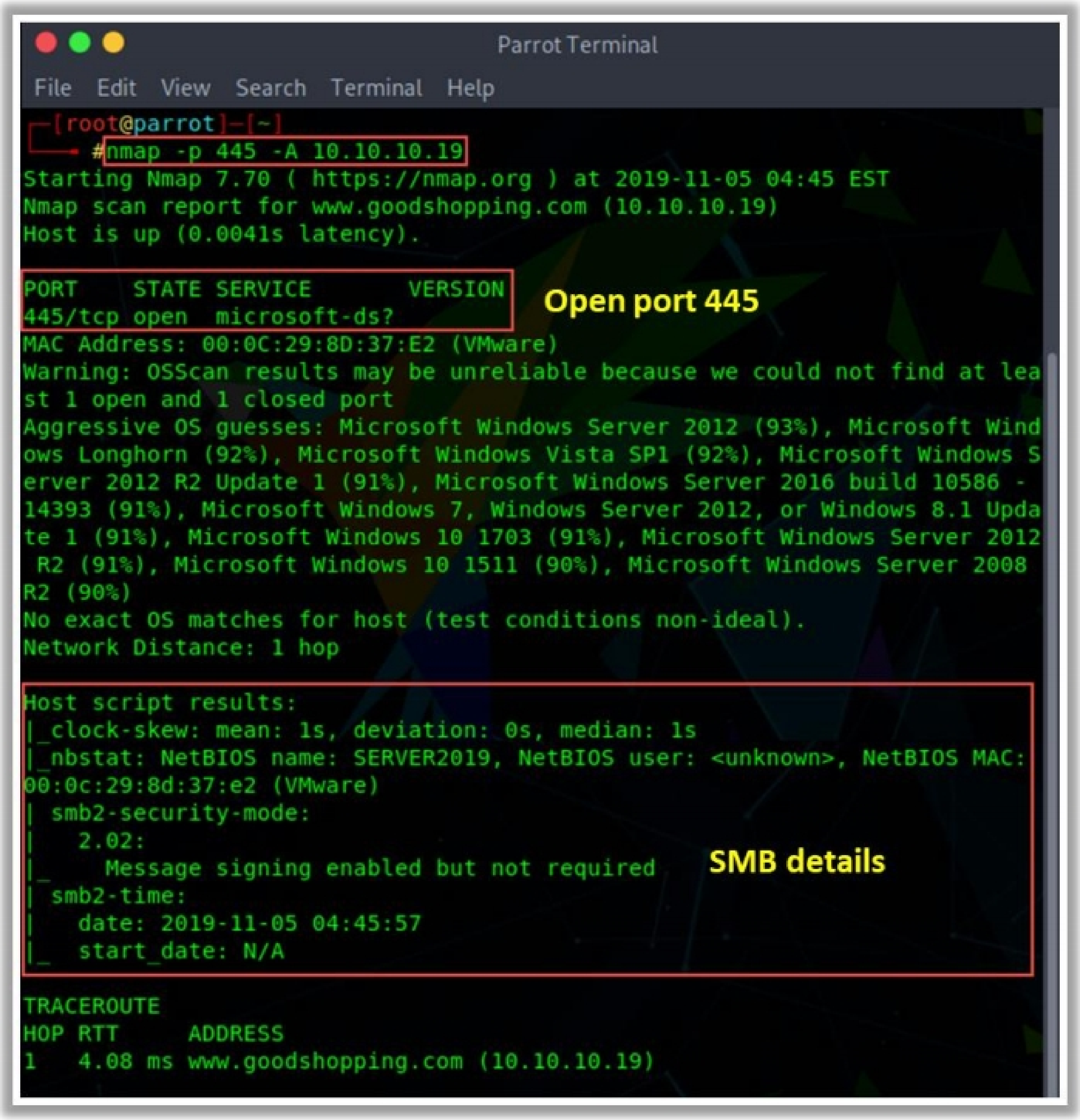
Server Message Block (SMB) is a transport protocol that is generally used by Windows systems for providing shared access to files, printers, and serial ports as well as remote access to Windows services. By default, SMB runs directly on TCP port 445 or via the NetBIOS API on UDP ports 137 and 138 and TCP ports 137 and 139. By using the SMB service, users can access files and other data stored at a remote server. The SMB service also allows application users to read, write, and modify the files on the remote server. A network running this service is highly vulnerable to SMB enumeration, which provides a good amount of information about the target.

In SMB enumeration, attackers generally perform banner grabbing to obtain information such as OS details and versions of services running. By using this information, attackers can perform various attacks such as SMB relay attacks and brute-force attacks. Attackers can also use SMB enumeration tools such as Nmap, SMBMap, enum4linux, nullinux, and NetScanTool Pro to perform a directed scan on the SMB service running on port 445.

As shown in the screenshot, attackers use the following Nmap command to enumerate the SMB service running on the target IP address:

```
# nmap -p 445 -A <target IP>
```

In the above command, the option `-p` specifies a port to scan (`445` in this case), and option `-A` is used for OS detection, version detection, script scanning, and traceroute information.



```
┌─[root@parrot]─[~]
└──╼ #nmap -p 445 -A 10.10.10.19
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-05 04:45 EST
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.0041s latency).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?
MAC Address: 00:0C:29:8D:37:E2 (VMware)
Warning: OSScan results may be unreliable because we could not find at lea
st 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 (93%), Microsoft Wind
ows Longhorn (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows S
erver 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 -
14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Upda
te 1 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows Server 2012
 R2 (91%), Microsoft Windows 10 1511 (90%), Microsoft Windows Server 2008
R2 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
|_nbstat: NetBIOS name: SERVER2019, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:8d:37:e2 (VMware)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-11-05 04:45:57
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   4.08 ms www.goodshopping.com (10.10.10.19)
```

Open port 445

SMB details

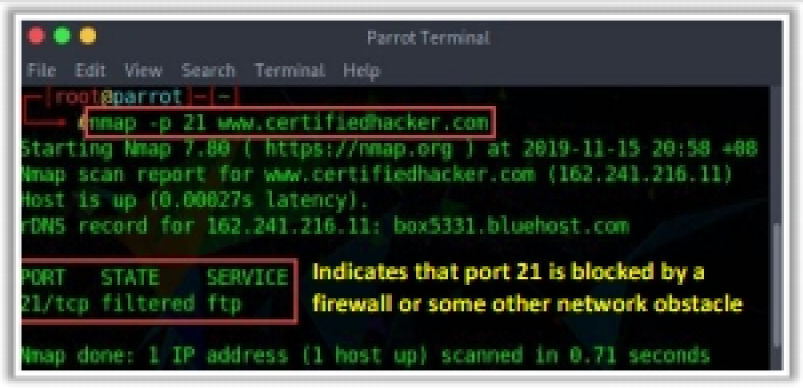
Figure 4.38: Screenshot of Nmap performing SMB enumeration

The **`STATE`** of **`PORT 445/tcp`** is **`OPEN`,** which indicates that port 445 is open and that the SMB service is running. By using this command, attackers can also obtain details on the OS and traceroute of the specified target.

FTP and TFTP Enumeration

FTP Enumeration

- FTP transfers data in plain text between the sender and receiver, which can lead to critical information, such as **usernames and passwords**, **being exposed to attackers**
- Attackers use **Nmap** to scan and enumerate open port 21 by running FTP services and further use the information to launch various attacks, such as **FTP bounce**, **FTP brute force**, and **packet sniffing**

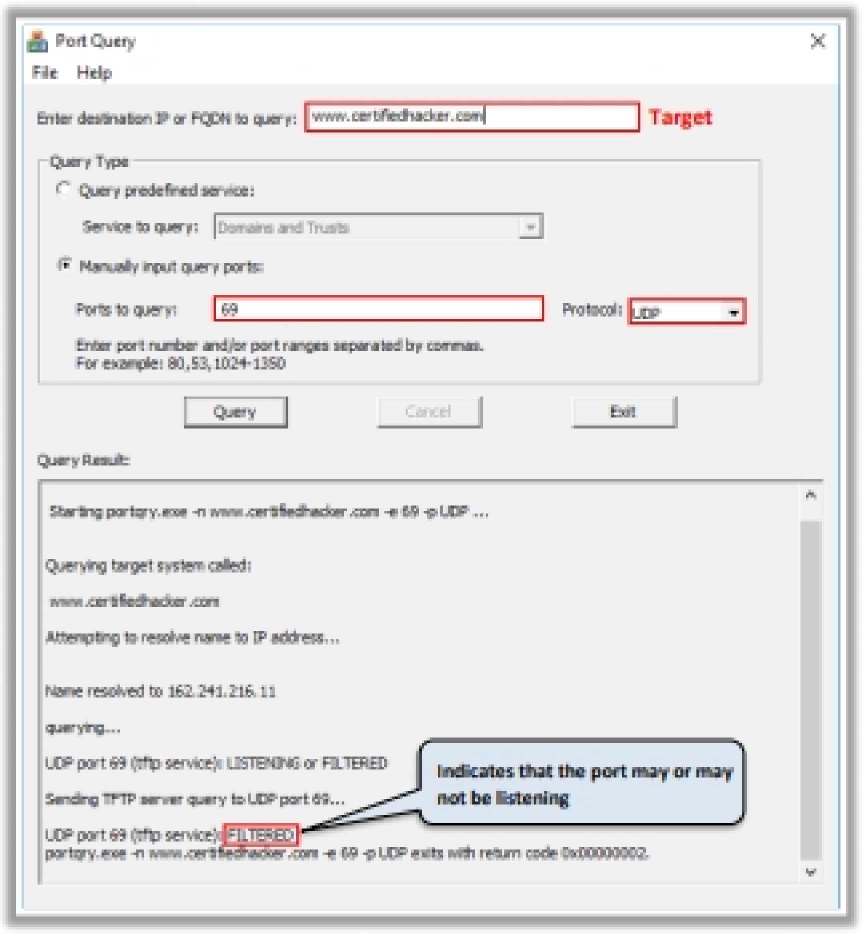


```
┌─[root@parrot]─[~]
└──╼ #nmap -p 21 www.certifiedhacker.com
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 20:58 +08
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.00027s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT    STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
```

Indicates that port 21 is blocked by a firewall or some other network obstacle

TFTP Enumeration

- Attackers perform TFTP enumeration using tools, such as **PortQry** and **Nmap**, to extract information, such as **running TFTP services** and files stored on the remote server
- Using this information, attackers can gain unauthorized access to the target system, steal important files, and upload malicious script to launch further attacks



Enter destination IP or FQDN to query: www.certifiedhacker.com

Target

Query Type

○ Query predefined service:

Service to query: Domains and Trusts

● Manually input query ports:

Ports to query: 69 Protocol: UDP

Enter port number and/or port ranges separated by commas.
For example: 80,53,1024-1350

Query Result:

```
Starting portqry.exe -n www.certifiedhacker.com -e 69 -p UDP ...


Querying target system called:

 www.certifiedhacker.com

Attempting to resolve name to IP address...


Name resolved to 162.241.216.11

querying...

UDP port 69 (tftp service): LISTENING or FILTERED

Sending TFTP server query to UDP port 69...

UDP port 69 (tftp service): FILTERED
portqry.exe -n www.certifiedhacker.com -e 69 -p UDP exits with return code 0x00000002.
```

Indicates that the port may or may not be listening

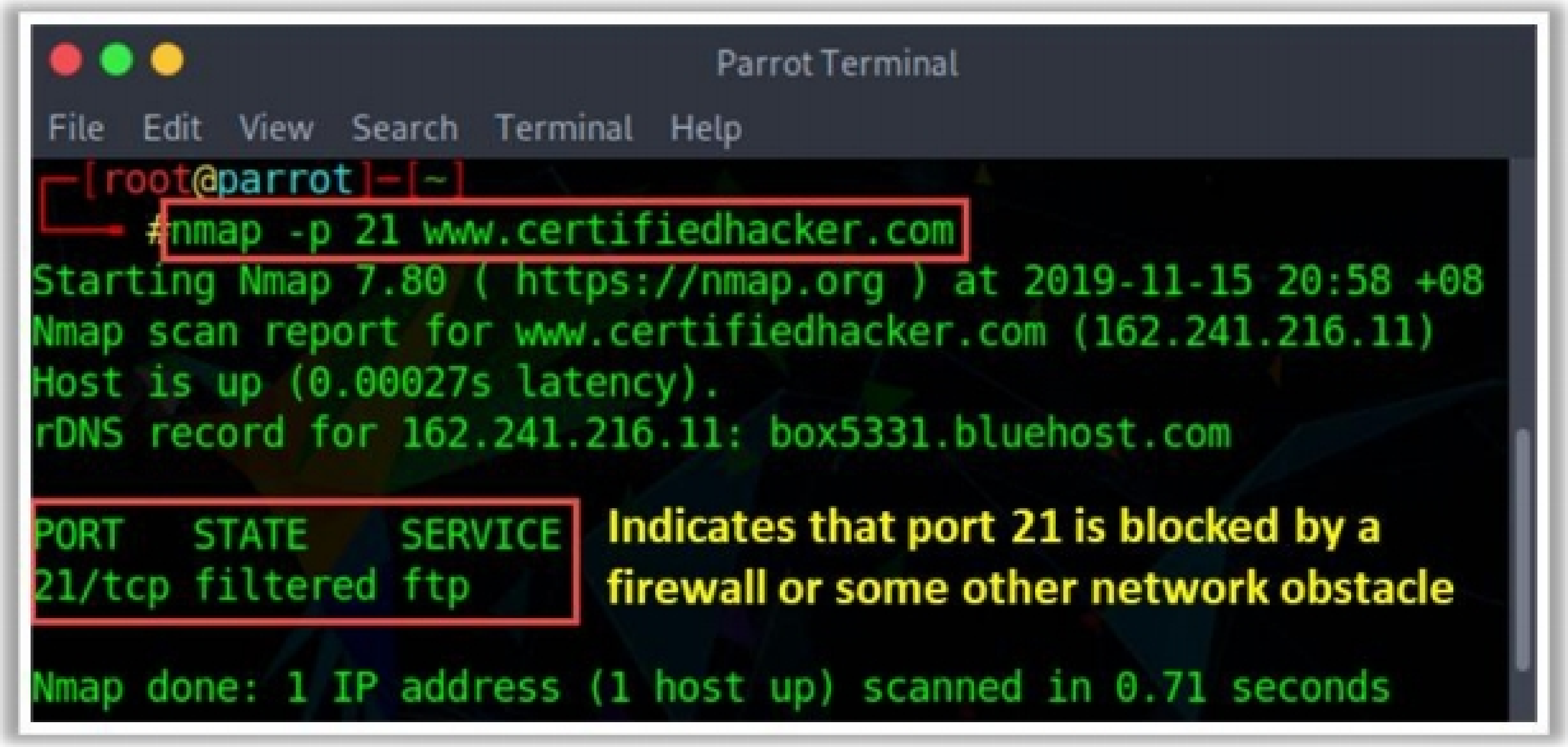
FTP Enumeration

The File Transfer Protocol (FTP) is used to transfer files over TCP, and its default port is 21. In FTP, data are transferred between a sender and receiver in plaintext, exposing critical information such as usernames and passwords to attackers. FTP offers neither a secure network environment nor secure user authentication. Individuals do not need authentication to access an FTP server in a network. This provides an easy method for attackers to access network resources.

The implementation of FTP in an organization's network makes the data accessible to external sources. Attackers can scan and enumerate open port 21 running FTP services and further use this information to launch various attacks such as FTP bounce, FTP brute force, and packet sniffing.

As shown in the screenshot, the following Nmap command is used by the attackers to enumerate the FTP service running on the target domain:

```
# nmap -p 21 <target domain>
```



```
┌─[root@parrot]─[~]
└──╼ #nmap -p 21 www.certifiedhacker.com
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 20:58 +08
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.00027s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
```

Indicates that port 21 is blocked by a firewall or some other network obstacle

Figure 4.39: Screenshot of Nmap displaying a FTP enumeration result

Attackers also use Metasploit to enumerate FTP services running on remote hosts. The following commands can be used to detect the FTP version of the target server:

```
use auxiliary/scanner/ftp/ftp_version
msf auxiliary(scanner/ftp/ftp_version) > set RHOSTS <target IP>
msf auxiliary(scanner/ftp/ftp_version) > exploit
```

TFTP Enumeration

The Trivial File Transfer Protocol (TFTP) is a simplified version of FTP and is used for transferring files between network devices. By default, TFTP servers listen on UDP port 69. This protocol is used when directory visibility and user authentication are not required; therefore, it provides no security features.

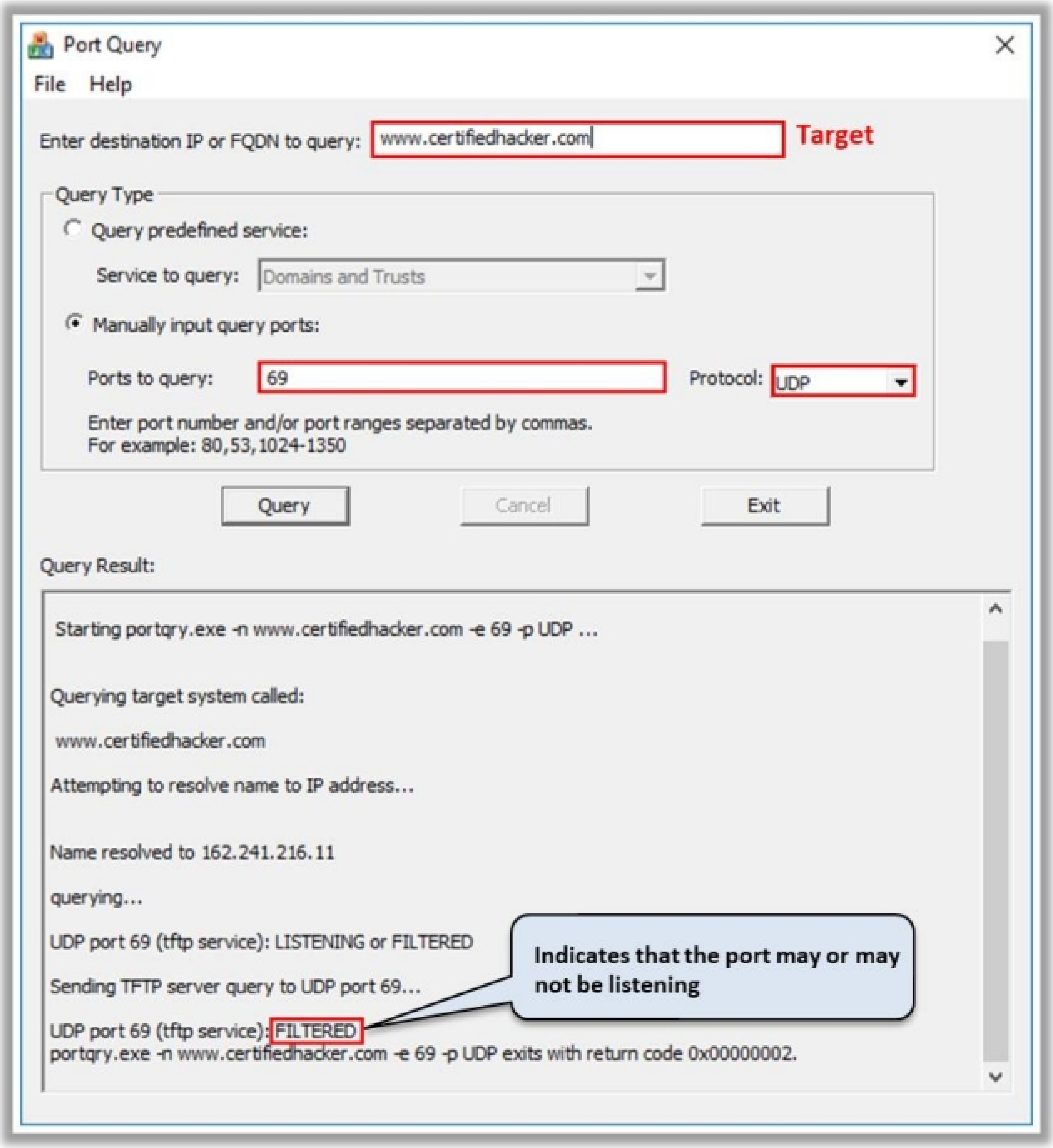
To perform TFTP enumeration, attackers can use tools such as PortQry and Nmap to extract information such as running TFTP services and files stored on a remote server. By using the enumerated information, attackers can further gain unauthorized access to the target system, steal important files, and upload malicious scripts to launch further attacks. Furthermore, this information enables attackers to perform various attacks such as DNS amplification attacks, TFTP reflection attacks, and DDoS attacks.

- **PortQry**

  Source: *https://www.microsoft.com*

  The PortQry utility reports the port status of TCP and UDP ports on a selected target. Attackers can use the PortQry tool to perform TFTP enumeration. This utility reports the port status of target TCP and UDP ports on a local or remote computer.

  In the PortQry tool, the attackers can specify the target to scan for a running TFTP service on open port 69. As shown in the screenshot, attackers perform TFTP enumeration on the target domain by setting the `Ports to query:` value to 69 and `Protocol` to UDP.


Port Query
File
Help
Target
Query Type
Service to query:
Domains and Trusts
Query
Cancel
Exit
Query Result:
Indicates that the port may or may not be listening

Enter destination IP or FQDN to query: www.certifiedhacker.com

○ Query predefined service:

● Manually input query ports:

Ports to query: 69

Protocol: UDP

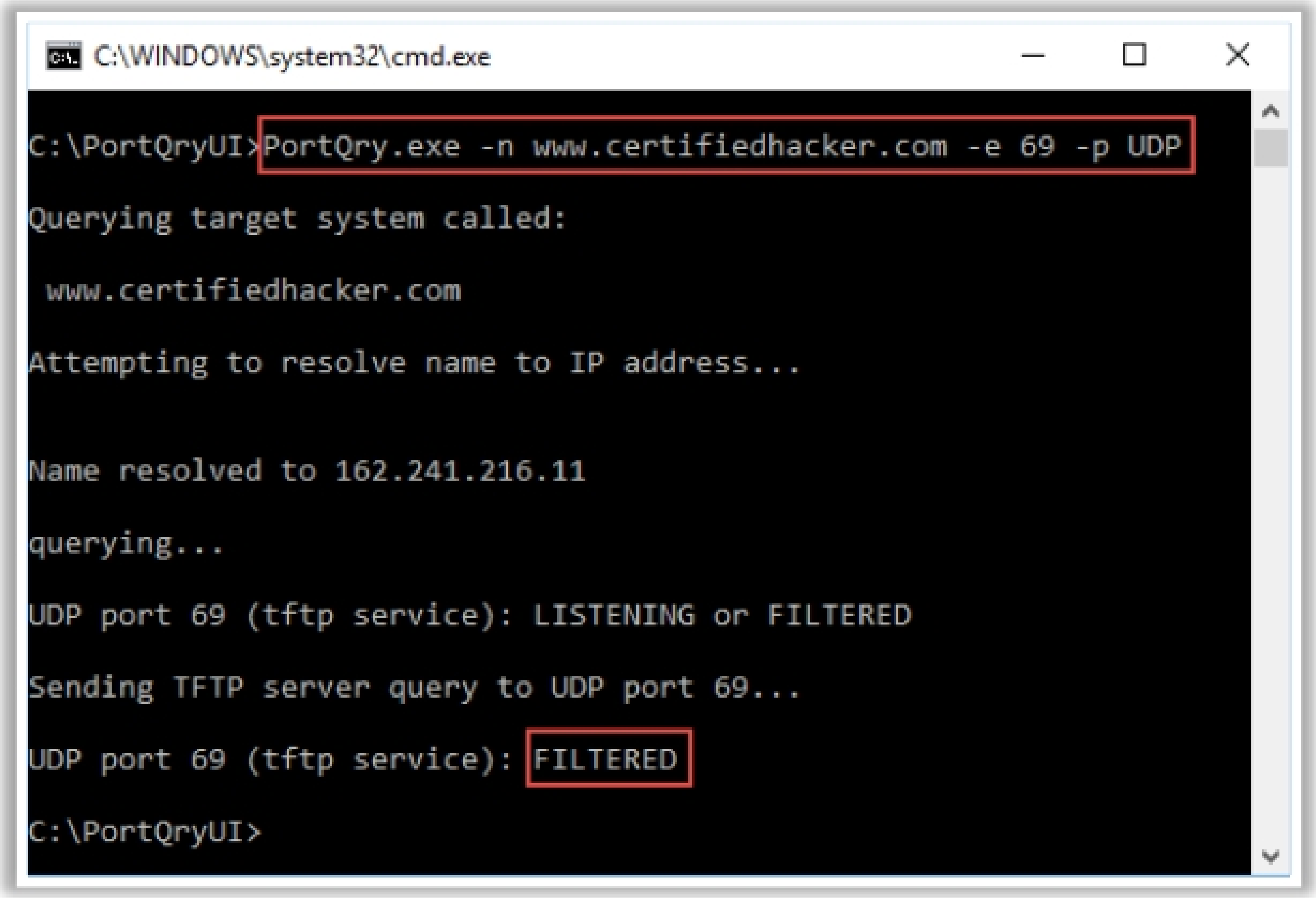
Enter port number and/or port ranges separated by commas.
For example: 80,53,1024-1350

```
Starting portqry.exe -n www.certifiedhacker.com -e 69 -p UDP ...


Querying target system called:

 www.certifiedhacker.com

Attempting to resolve name to IP address...


Name resolved to 162.241.216.11

querying...

UDP port 69 (tftp service): LISTENING or FILTERED

Sending TFTP server query to UDP port 69...

UDP port 69 (tftp service): FILTERED
portqry.exe -n www.certifiedhacker.com -e 69 -p UDP exits with return code 0x00000002.
```

Figure 4.40: Screenshot of the PortQry tool displaying a TFTP scan result

Attackers can also use the PortQry command-line utility to perform TFTP enumeration using the following command:

`portqry -n <target domain> -e 69 -p udp`



```
C:\PortQryUI>PortQry.exe -n www.certifiedhacker.com -e 69 -p UDP
Querying target system called:
 www.certifiedhacker.com
Attempting to resolve name to IP address...

Name resolved to 162.241.216.11
querying...
UDP port 69 (tftp service): LISTENING or FILTERED
Sending TFTP server query to UDP port 69...
UDP port 69 (tftp service): FILTERED
C:\PortQryUI>
```

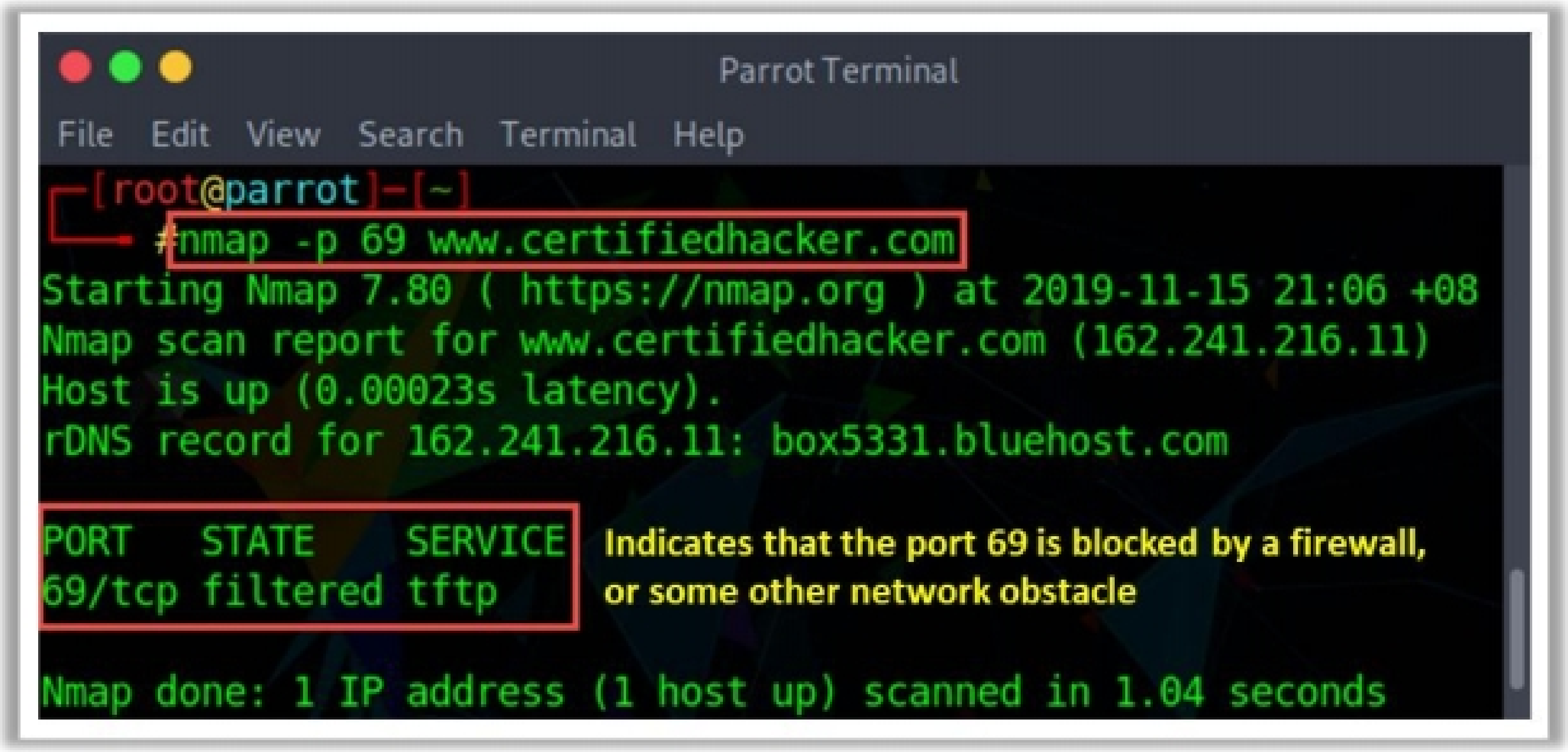
Figure 4.41: Screenshot of the PortQry command-line utility showing a TFTP scan result

- **Nmap**

  Source: *https://nmap.org*

  Attackers can use the Nmap tool to perform simple direct scanning for TFTP port 69. As shown in the screenshot, the following Nmap command is used by attackers to enumerate the TFTP service running on the target domain:

  `# nmap -p 69 <target domain>`



```
┌─[root@parrot]─[~]
└──╼ #nmap -p 69 www.certifiedhacker.com
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 21:06 +08
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.00023s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT    STATE    SERVICE
69/tcp filtered tftp

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
```

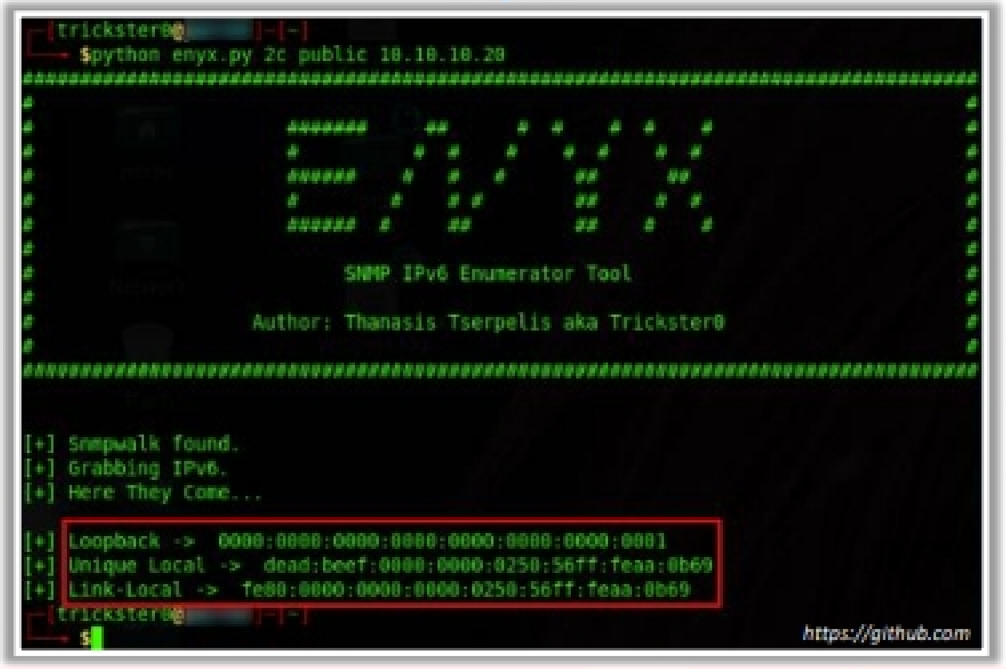
Indicates that the port 69 is blocked by a firewall, or some other network obstacle

Figure 4.42: Screenshot of Nmap command displaying a TFTP scan result

IPv6 Enumeration

- IPv6 is an addressing protocol that **provides identification to computer systems**, including their location information and further assists in routing traffic from one system to the other across the network
- Attackers perform IPv6 enumeration using various tools, such as Enyx and IPv6 Hackit, on target hosts to **obtain their IPv6 addresses** and further scan the enumerated IP addresses to detect various security problems

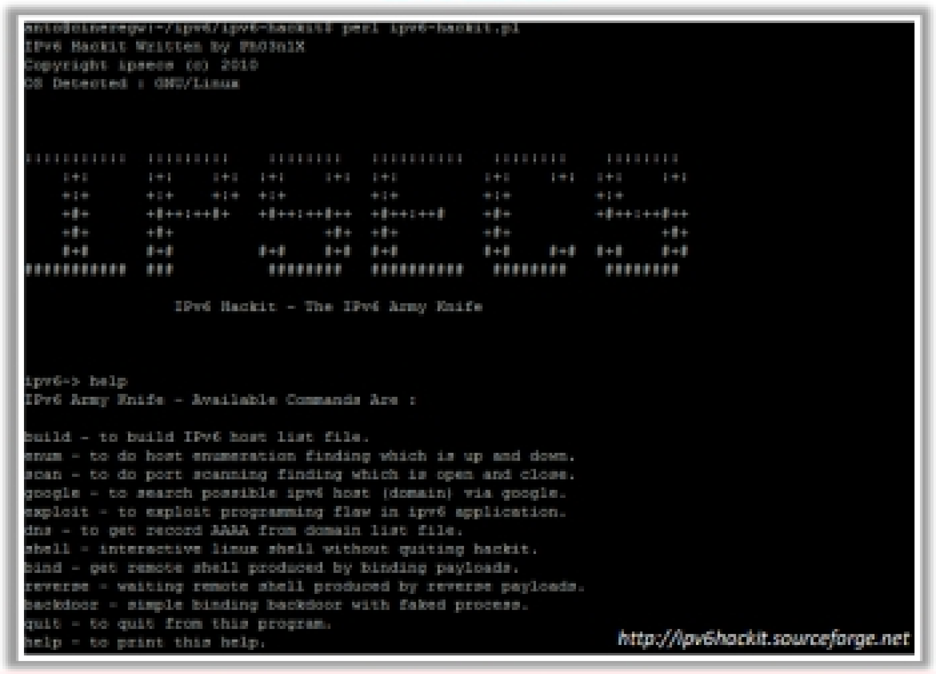
Enyx



```
┌─[trickster0@[redacted]]─[~]
└──╼ $python enyx.py 2c public 10.10.10.20

                    SNMP IPv6 Enumerator Tool

            Author: Thanasis Tserpelis aka Trickster0

[+] Snmpwalk found.
[+] Grabbing IPv6.
[+] Here They Come...

[+] Loopback ->  0000:0000:0000:0000:0000:0000:0000:0001
[+] Unique Local ->  dead:beef:0000:0000:0250:56ff:feaa:0b69
[+] Link-Local ->  fe80:0000:0000:0000:0250:56ff:feaa:0b69
┌─[trickster0@[redacted]]─[~]
└──╼ $
```

https://github.com

IPv6 Hackit



```
anto@dineregw:~/ipv6/ipv6-hackit$ perl ipv6-hackit.pl
IPv6 Hackit Written by Ph03n1X
Copyright ipsecs (c) 2010
OS Detected : GNU/Linux

                IPv6 Hackit - The IPv6 Army Knife

ipv6-> help
IPv6 Army Knife - Available Commands Are :

build - to build IPv6 host list file.
enum - to do host enumeration finding which is up and down.
scan - to do port scanning finding which is open and close.
google - to search possible ipv6 host (domain) via google.
exploit - to exploit programming flaw in ipv6 application.
dns - to get record AAAA from domain list file.
shell - interactive linux shell without quiting hackit.
bind - get remote shell produced by binding payloads.
reverse - waiting remote shell produced by reverse payloads.
backdoor - simple binding backdoor with faked process.
quit - to quit from this program.
help - to print this help.
```

http://ipv6hackit.sourceforge.net

IPv6 Enumeration

Internet Protocol version 6 (IPv6) is an addressing protocol that identifies computer systems, including location information, and assists in routing traffic from one system to another system across a network. It is an advanced version of IPv4 and, therefore, supports a greater number of hosts as compared to IPv4. It was designed to overcome the problem of IPv4 address exhaustion.

Attackers perform IPv6 enumeration on target hosts to obtain their IPv6 addresses and further scan the enumerated IP addresses to detect various security problems such as access to routing structure, exposure of sensitive content, and users' access control lists. By using this information, attackers can launch various attacks such as SYN flood attacks, DNS amplification attacks, and DDoS attacks. Attackers can scan and enumerate the IPv6 address of a target machine in the network by using various tools such as Enyx and IPv6 Hackit.

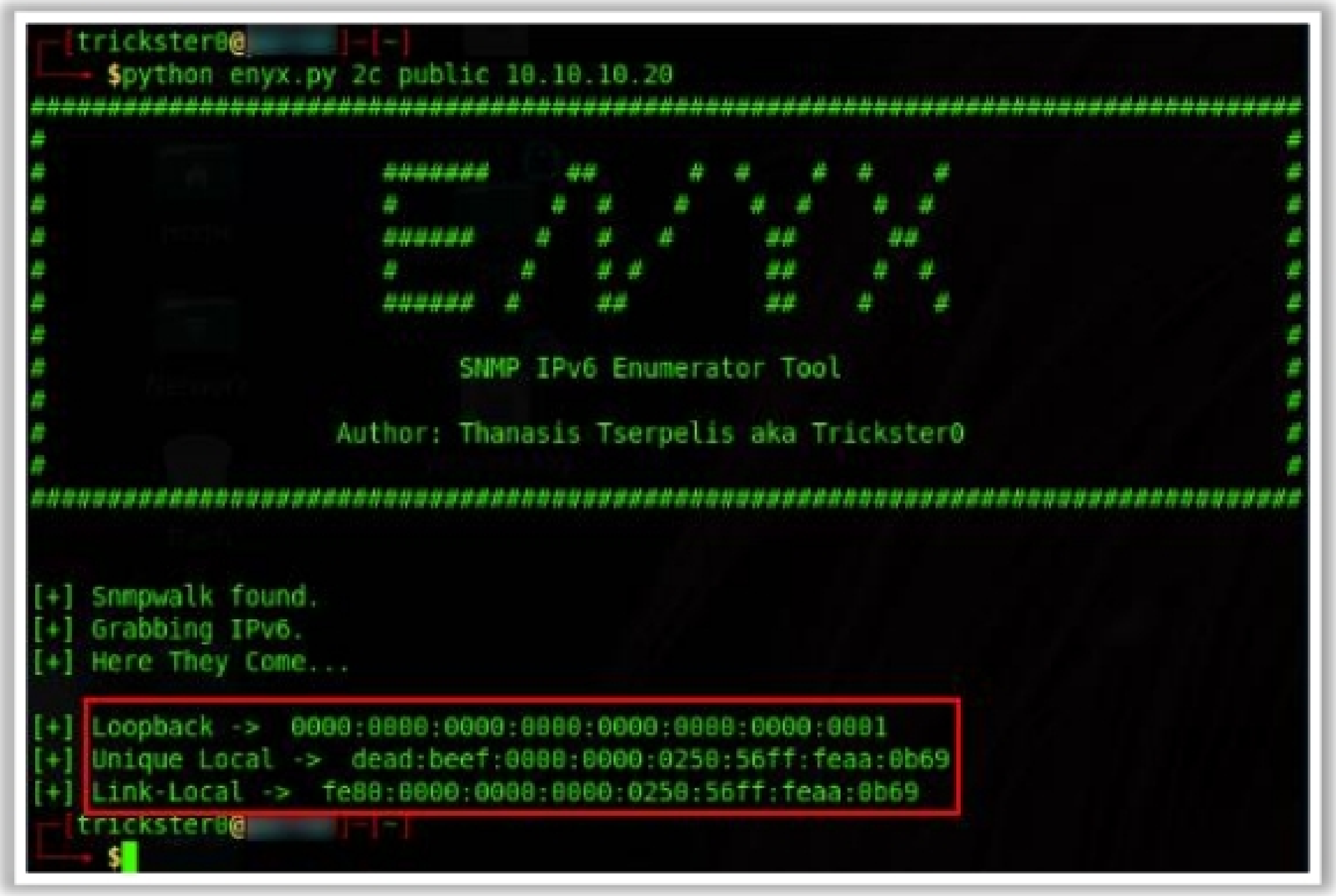
- **Enyx**

  Source: *https://github.com*

  Enyx is an enumeration tool that fetches the IPv6 address of a machine through SNMP.

  As shown in the screenshot, attackers use the following command to enumerate the IPv6 address of a target machine (`10.10.10.20`) by setting the SNMP version to **`2c`** and community string to **`public`**:

  ```
  Python enyx.py 2c public <target IP>
  ```



```
┌─[trickster0@[redacted]]─[~]
└──╼ $python enyx.py 2c public 10.10.10.20
###########################################################################################
#                                                                                         #
#                  #######    ##     # #    # #    #                                      #
#                  #         # #    #    # #    # #                                       #
#                  ######   #  #   #      ##     ##                                       #
#                  #       #   # #        ##    # #                                       #
#                  ###### #    ##         ##   #   #                                      #
#                                                                                         #
#                         SNMP IPv6 Enumerator Tool                                       #
#                                                                                         #
#                  Author: Thanasis Tserpelis aka Trickster0                              #
#                                                                                         #
###########################################################################################


[+] Snmpwalk found.
[+] Grabbing IPv6.
[+] Here They Come...

[+] Loopback ->  0000:0000:0000:0000:0000:0000:0000:0001
[+] Unique Local ->  dead:beef:0000:0000:0250:56ff:feaa:0b69
[+] Link-Local ->  fe80:0000:0000:0000:0250:56ff:feaa:0b69
┌─[trickster0@[redacted]]─[~]
└──╼ $
```

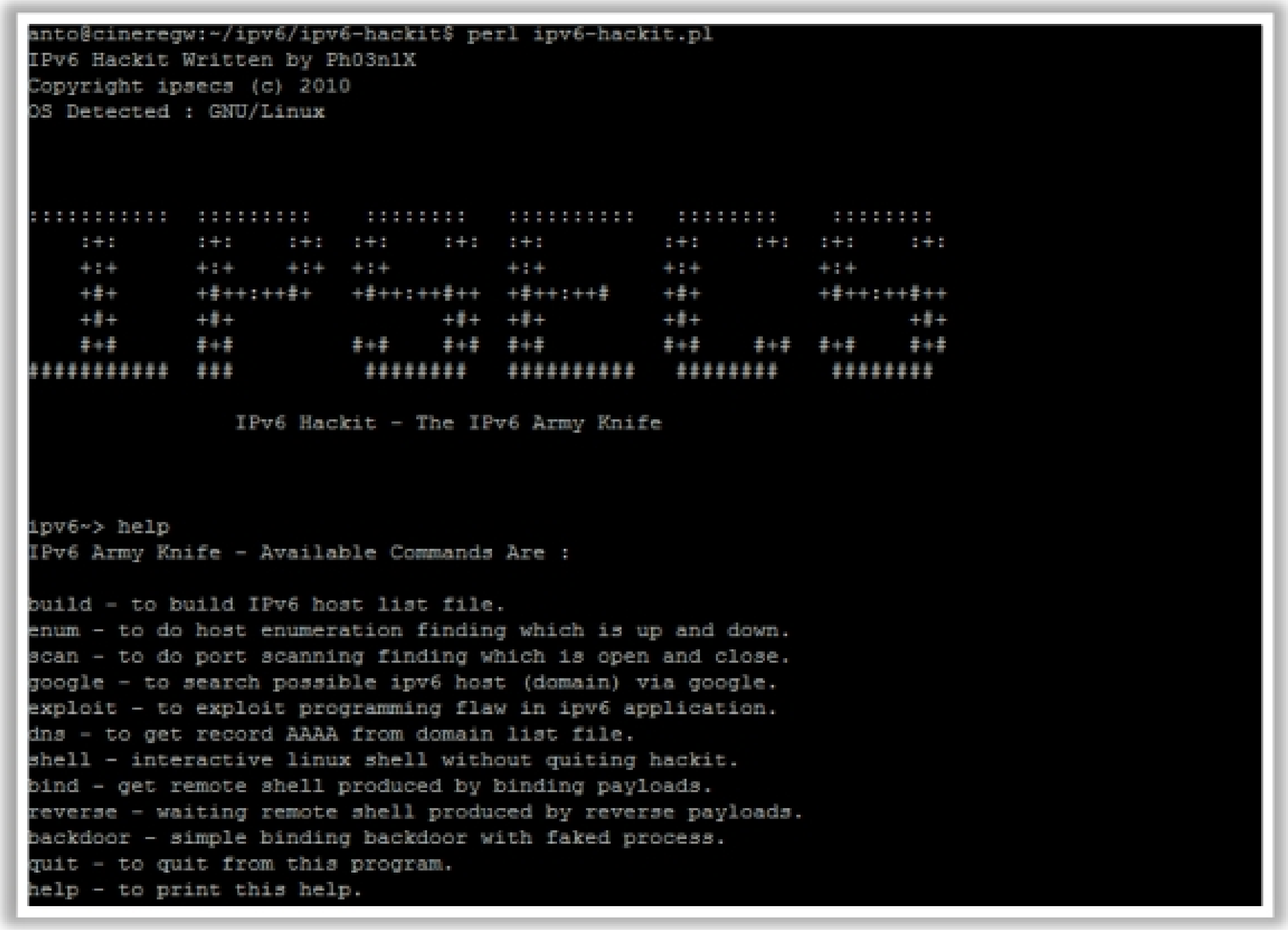
Figure 4.43: Screenshot of Enyx tool displaying enumerated results

- **IPv6 Hackit**

  Source: *http://ipv6hackit.sourceforge.net*

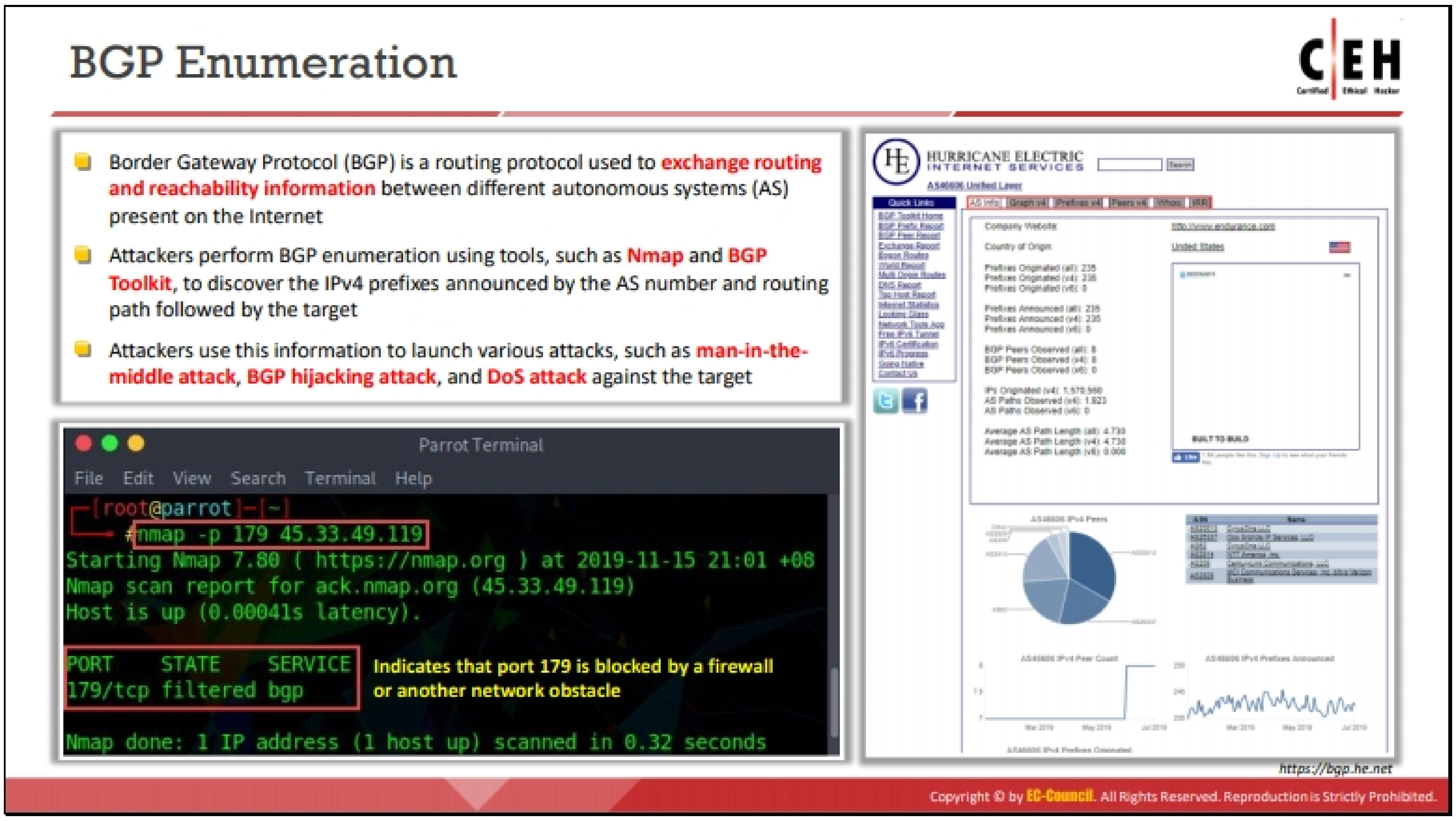
  Hackit is a scanning tool that provides a list of active IPv6 hosts. It can perform TCP port scanning and identify AAAA IPv6 host records.

  As shown in the screenshot, attackers can specify the target machine and run a scan to enumerate the IPv6 information.



```
anto@cineregw:~/ipv6/ipv6-hackit$ perl ipv6-hackit.pl
IPv6 Hackit Written by Ph03n1X
Copyright ipsecs (c) 2010
OS Detected : GNU/Linux



:::::::::::  :::::::::    ::::::::    ::::::::::   ::::::::    ::::::::
    :+:      :+:    :+:  :+:    :+:   :+:         :+:    :+:  :+:    :+:
    +:+      +:+    +:+  +:+          +:+         +:+         +:+
    +#+      +#++:++#+   +#++:++#++   +#++:++#    +#+         +#++:++#++
    +#+      +#+                +#+   +#+         +#+                +#+
    #+#      #+#         #+#    #+#   #+#         #+#    #+#  #+#    #+#
###########  ###          ########    ##########   ########    ########

                IPv6 Hackit - The IPv6 Army Knife



ipv6~> help
IPv6 Army Knife - Available Commands Are :

build - to build IPv6 host list file.
enum - to do host enumeration finding which is up and down.
scan - to do port scanning finding which is open and close.
google - to search possible ipv6 host (domain) via google.
exploit - to exploit programming flaw in ipv6 application.
dns - to get record AAAA from domain list file.
shell - interactive linux shell without quiting hackit.
bind - get remote shell produced by binding payloads.
reverse - waiting remote shell produced by reverse payloads.
backdoor - simple binding backdoor with faked process.
quit - to quit from this program.
help - to print this help.
```

Figure 4.44: Screenshot displaying the IPv6 Hackit tool



BGP Enumeration

- Border Gateway Protocol (BGP) is a routing protocol used to **exchange routing and reachability information** between different autonomous systems (AS) present on the Internet
- Attackers perform BGP enumeration using tools, such as **Nmap** and **BGP Toolkit**, to discover the IPv4 prefixes announced by the AS number and routing path followed by the target
- Attackers use this information to launch various attacks, such as **man-in-the-middle attack**, **BGP hijacking attack**, and **DoS attack** against the target

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[root@parrot]─[~]
└──╼ #nmap -p 179 45.33.49.119
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 21:01 +08
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.00041s latency).

PORT    STATE    SERVICE
179/tcp filtered bgp

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

Indicates that port 179 is blocked by a firewall or another network obstacle

https://bgp.he.net

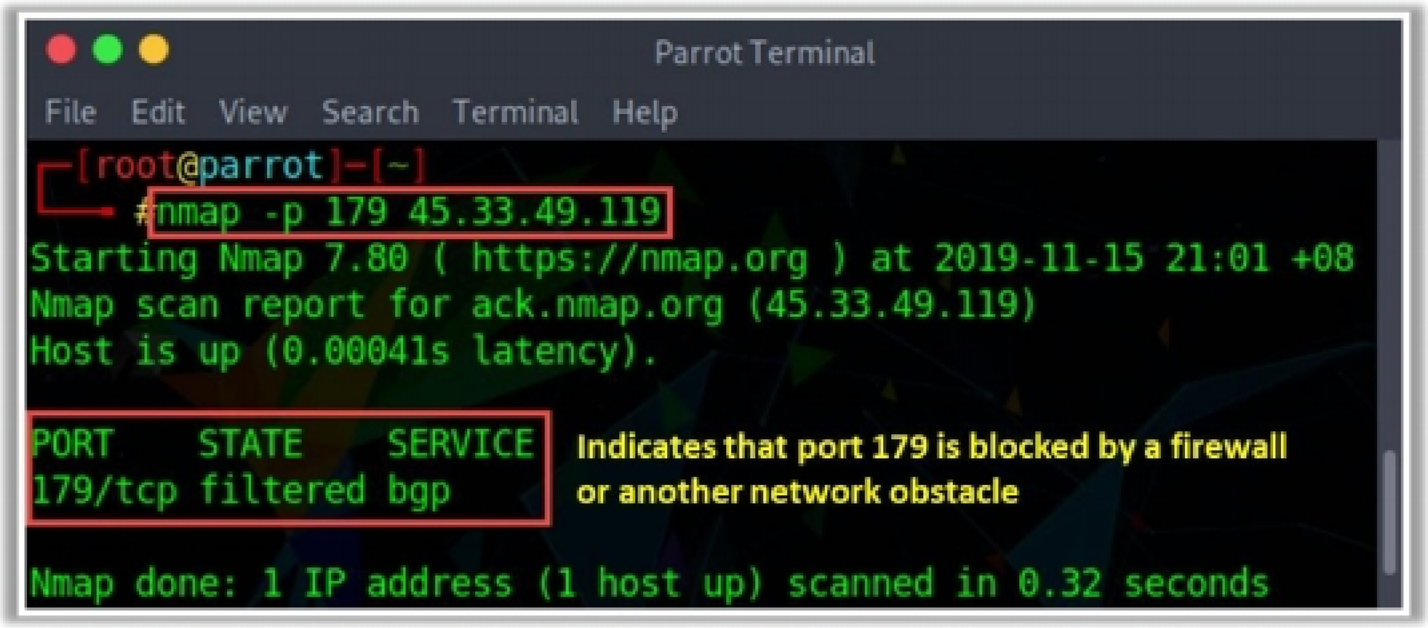
BGP Enumeration

The Border Gateway Protocol (BGP) is a routing protocol used to exchange routing and reachability information between different autonomous systems (AS) on the Internet. Because this protocol is used to connect one AS to other ASs, it is also called external BGP (eBGP). BGP finds the shortest path to route traffic from one IP address to another efficiently. BGP creates its TCP session on port 179.

Attackers perform BGP enumeration on the target using tools such as Nmap and BGP Toolkit to discover the IPv4 prefixes indicated by the AS number and the routing path followed by the target. Attackers use this information to launch various attacks against the target, such as man-in-the-middle attacks, BGP hijacking attacks, and DoS attacks.

As shown in the screenshot, attackers use the following Nmap command to enumerate BGP running on the target system:

```
# nmap -p 179 <target IP>
```

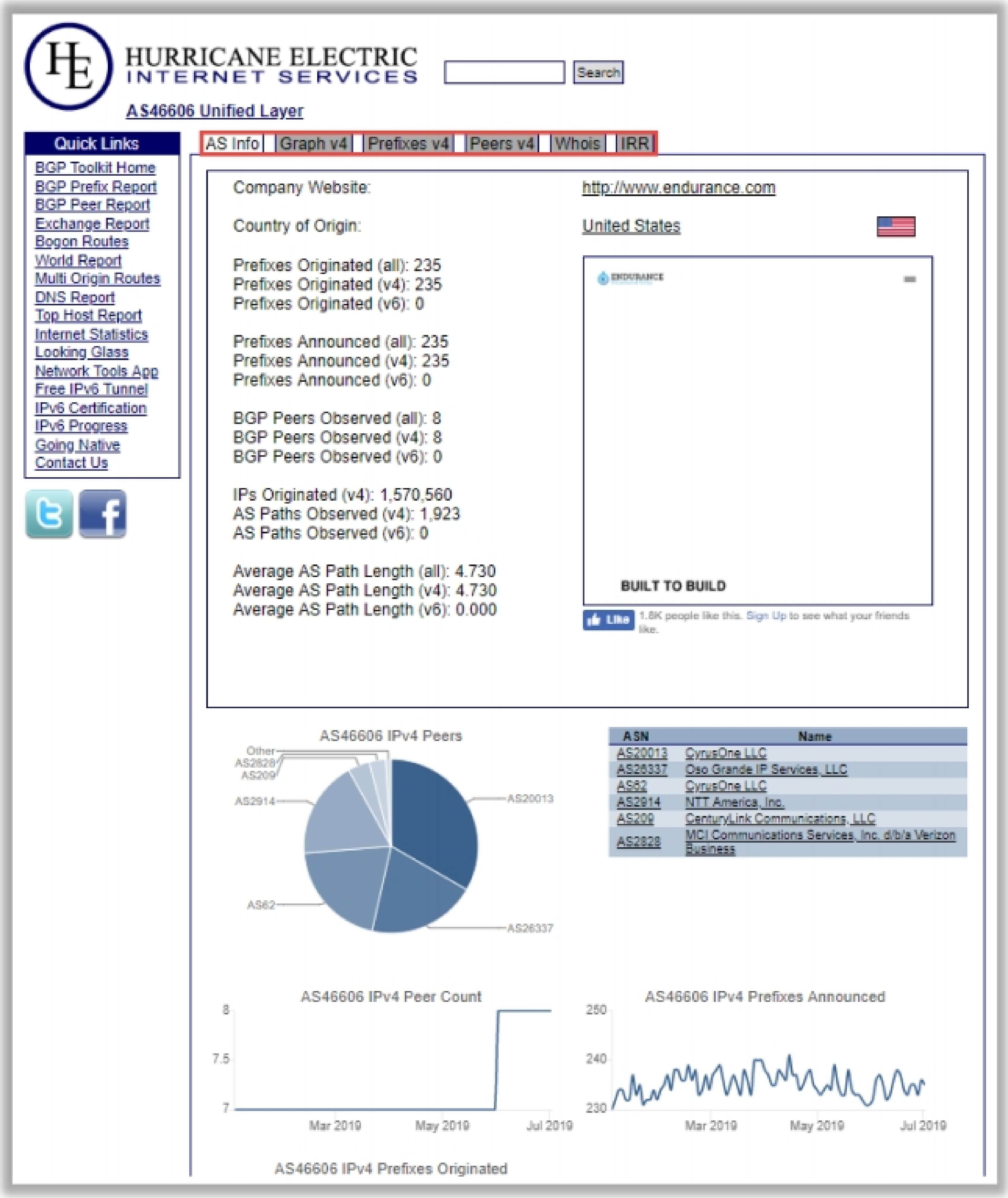


```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[root@parrot]─[~]
└──╼ #nmap -p 179 45.33.49.119
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 21:01 +08
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.00041s latency).

PORT    STATE    SERVICE
179/tcp filtered bgp

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

Indicates that port 179 is blocked by a firewall or another network obstacle

Figure 4.45: Screenshot of Nmap displaying a BGP enumeration result

As shown in the screenshot, attackers use BGP Toolkit to perform BGP enumeration on the target domain. This online tool can be used to search for the target domain and obtain details such as DNS information, website information, IP information, AS information, and whois information. Based on the identified ASs, attackers can further enumerate details such as IPv4 prefixes, BGP routing graphs, and IPv4 peers.


HURRICANE ELECTRIC
INTERNET SERVICES
Search
AS46606 Unified Layer
Quick Links
BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Exchange Report
Bogon Routes
World Report
Multi Origin Routes
DNS Report
Top Host Report
Internet Statistics
Looking Glass
Network Tools App
Free IPv6 Tunnel
IPv6 Certification
IPv6 Progress
Going Native
Contact Us
AS Info
Graph v4
Prefixes v4
Peers v4
Whois
IRR
ENDURANCE
BUILT TO BUILD
Like
1.8K people like this. Sign Up to see what your friends like.
AS46606 IPv4 Peers
Other
AS2828
AS209
AS2914
AS20013
AS62
AS26337
AS46606 IPv4 Peer Count
8
7.5
7
Mar 2019
May 2019
Jul 2019
AS46606 IPv4 Prefixes Announced
250
240
230
Mar 2019
May 2019
Jul 2019
AS46606 IPv4 Prefixes Originated

Company Website: http://www.endurance.com

Country of Origin: United States

Prefixes Originated (all): 235
Prefixes Originated (v4): 235
Prefixes Originated (v6): 0

Prefixes Announced (all): 235
Prefixes Announced (v4): 235
Prefixes Announced (v6): 0

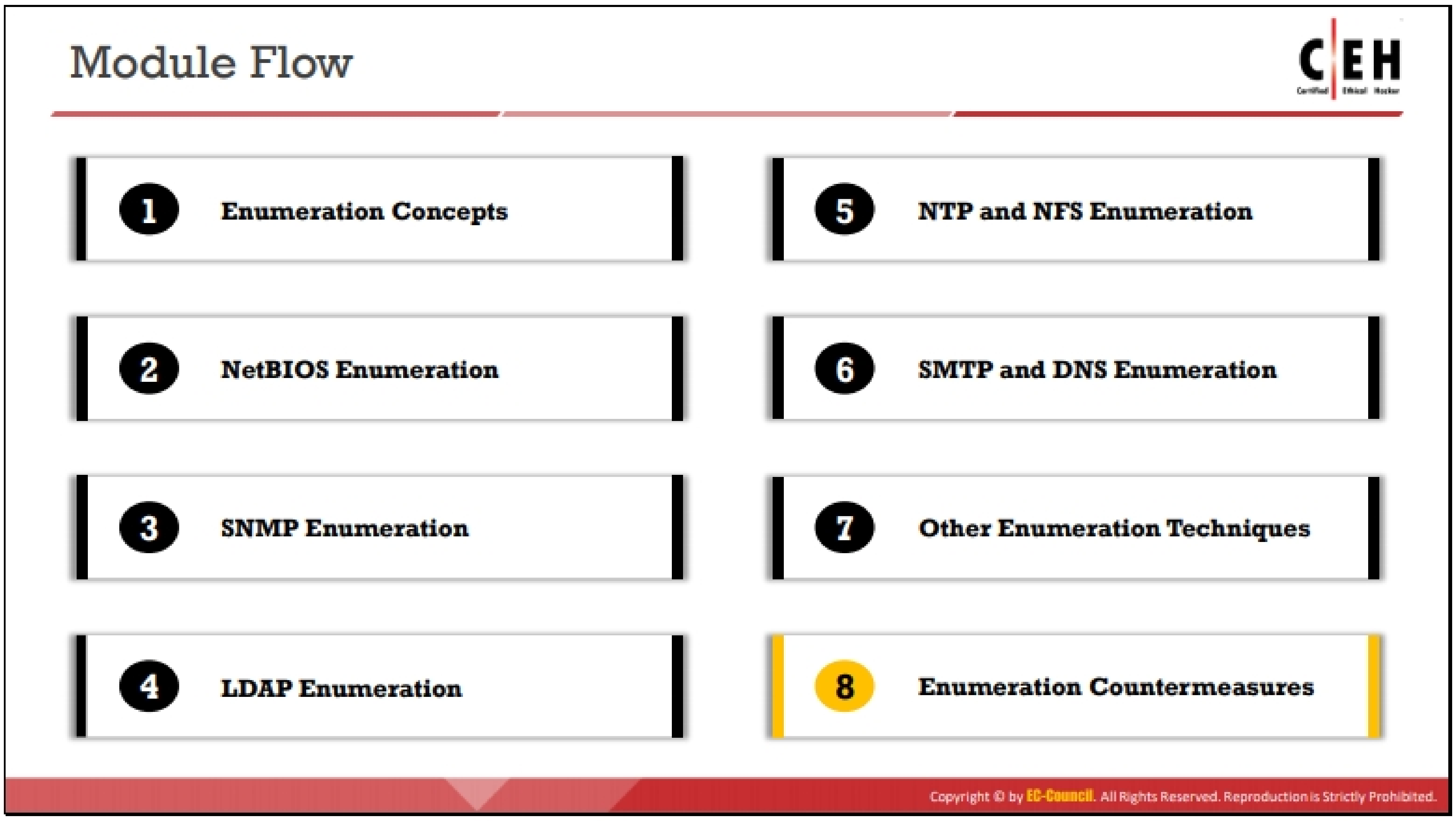
BGP Peers Observed (all): 8
BGP Peers Observed (v4): 8
BGP Peers Observed (v6): 0

IPs Originated (v4): 1,570,560
AS Paths Observed (v4): 1,923
AS Paths Observed (v6): 0

Average AS Path Length (all): 4.730
Average AS Path Length (v4): 4.730
Average AS Path Length (v6): 0.000

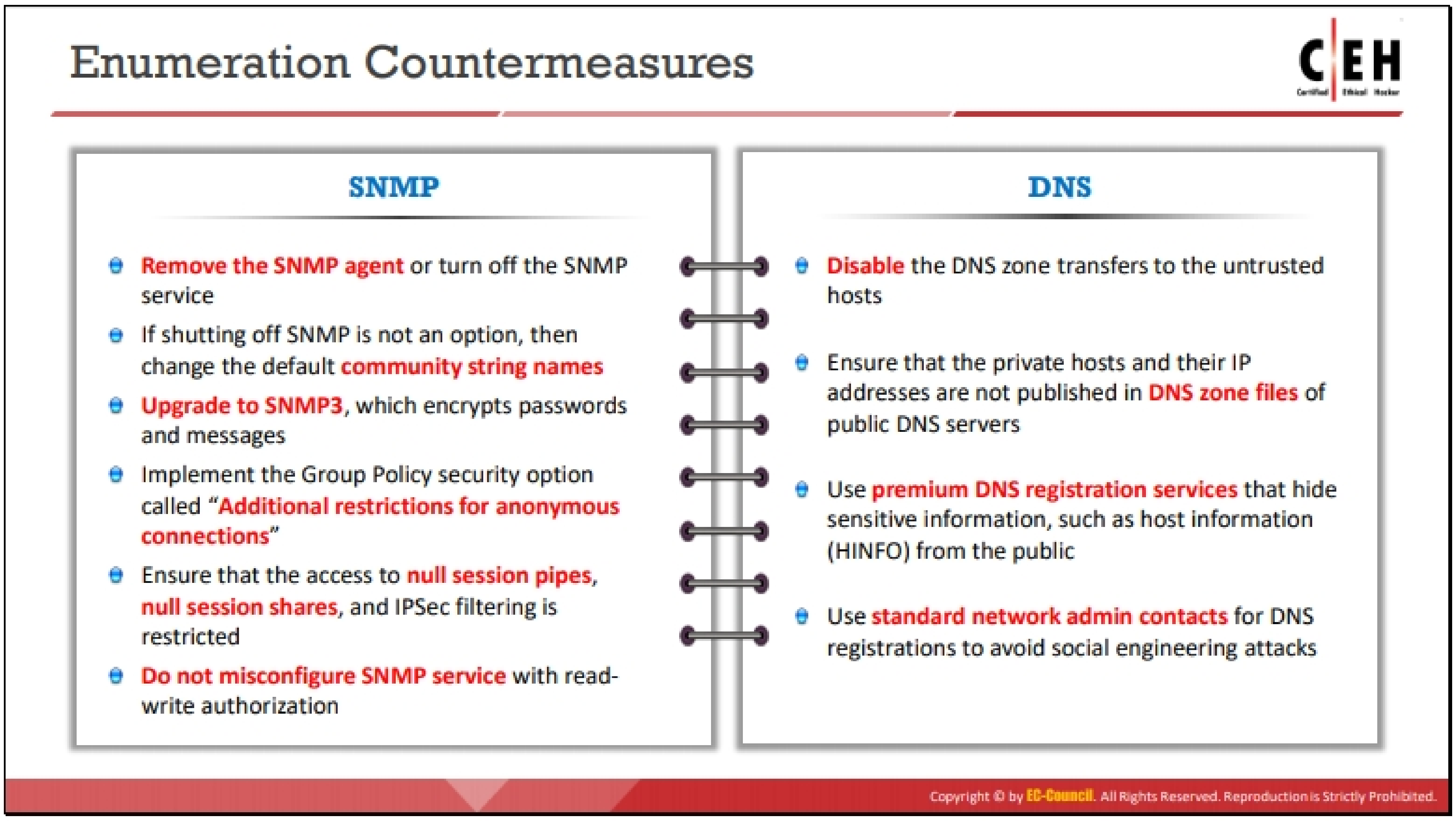
ASN	Name
AS20013	CyrusOne LLC
AS26337	Oso Grande IP Services, LLC
AS62	CyrusOne LLC
AS2914	NTT America, Inc.
AS209	CenturyLink Communications, LLC
AS2828	MCI Communications Services, Inc. d/b/a Verizon Business

Figure 4.46: Screenshot of BGP Toolkit



Module Flow

1. **Enumeration Concepts**
2. **NetBIOS Enumeration**
3. **SNMP Enumeration**
4. **LDAP Enumeration**
5. **NTP and NFS Enumeration**
6. **SMTP and DNS Enumeration**
7. **Other Enumeration Techniques**
8. **Enumeration Countermeasures**



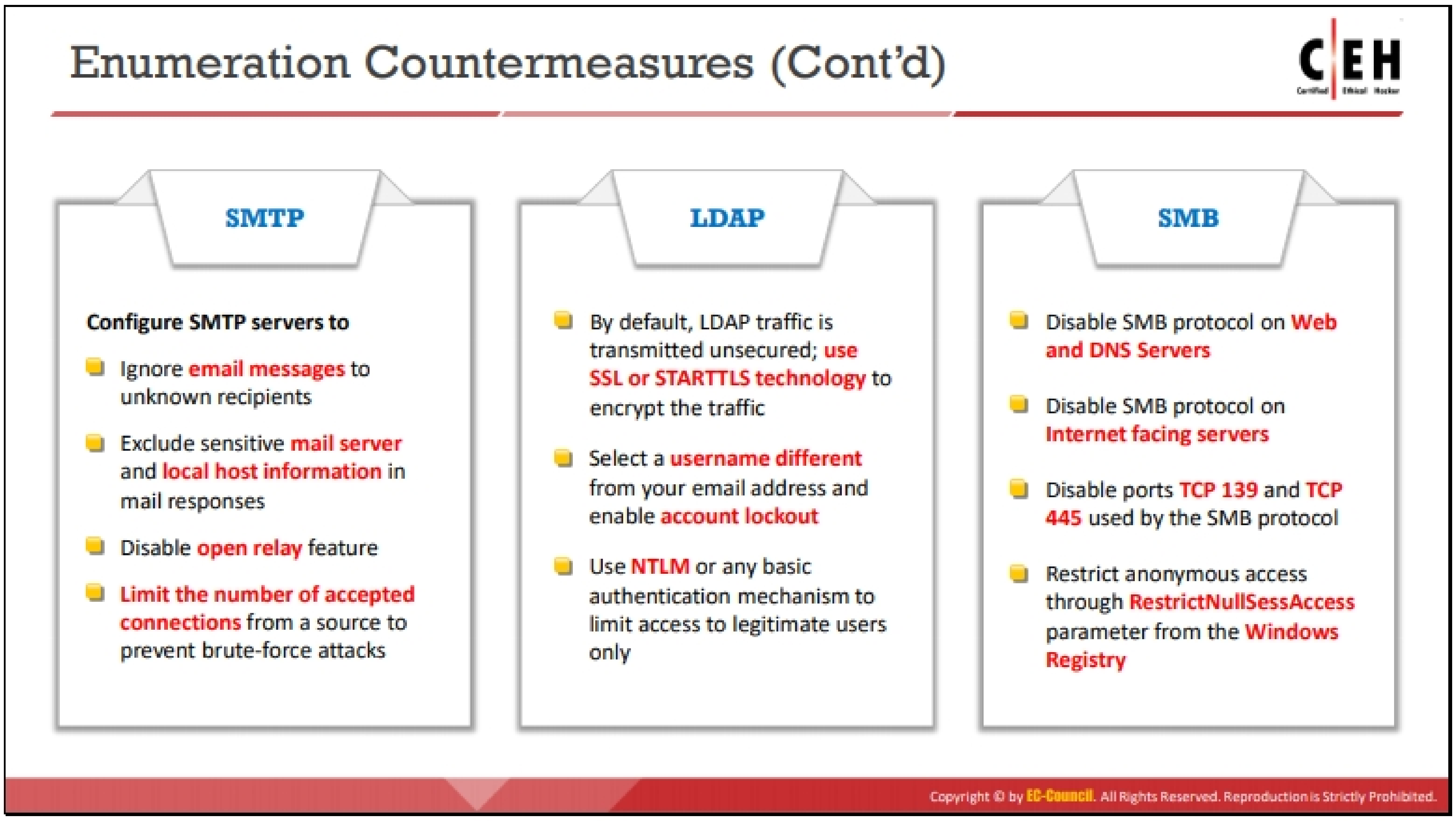
Enumeration Countermeasures

SNMP

- **Remove the SNMP agent** or turn off the SNMP service
- If shutting off SNMP is not an option, then change the default **community string names**
- **Upgrade to SNMP3**, which encrypts passwords and messages
- Implement the Group Policy security option called "**Additional restrictions for anonymous connections**"
- Ensure that the access to **null session pipes**, **null session shares**, and IPSec filtering is restricted
- **Do not misconfigure SNMP service** with read-write authorization

DNS

- **Disable** the DNS zone transfers to the untrusted hosts
- Ensure that the private hosts and their IP addresses are not published in **DNS zone files** of public DNS servers
- Use **premium DNS registration services** that hide sensitive information, such as host information (HINFO) from the public
- Use **standard network admin contacts** for DNS registrations to avoid social engineering attacks



Enumeration Countermeasures (Cont'd)

SMTP

Configure SMTP servers to

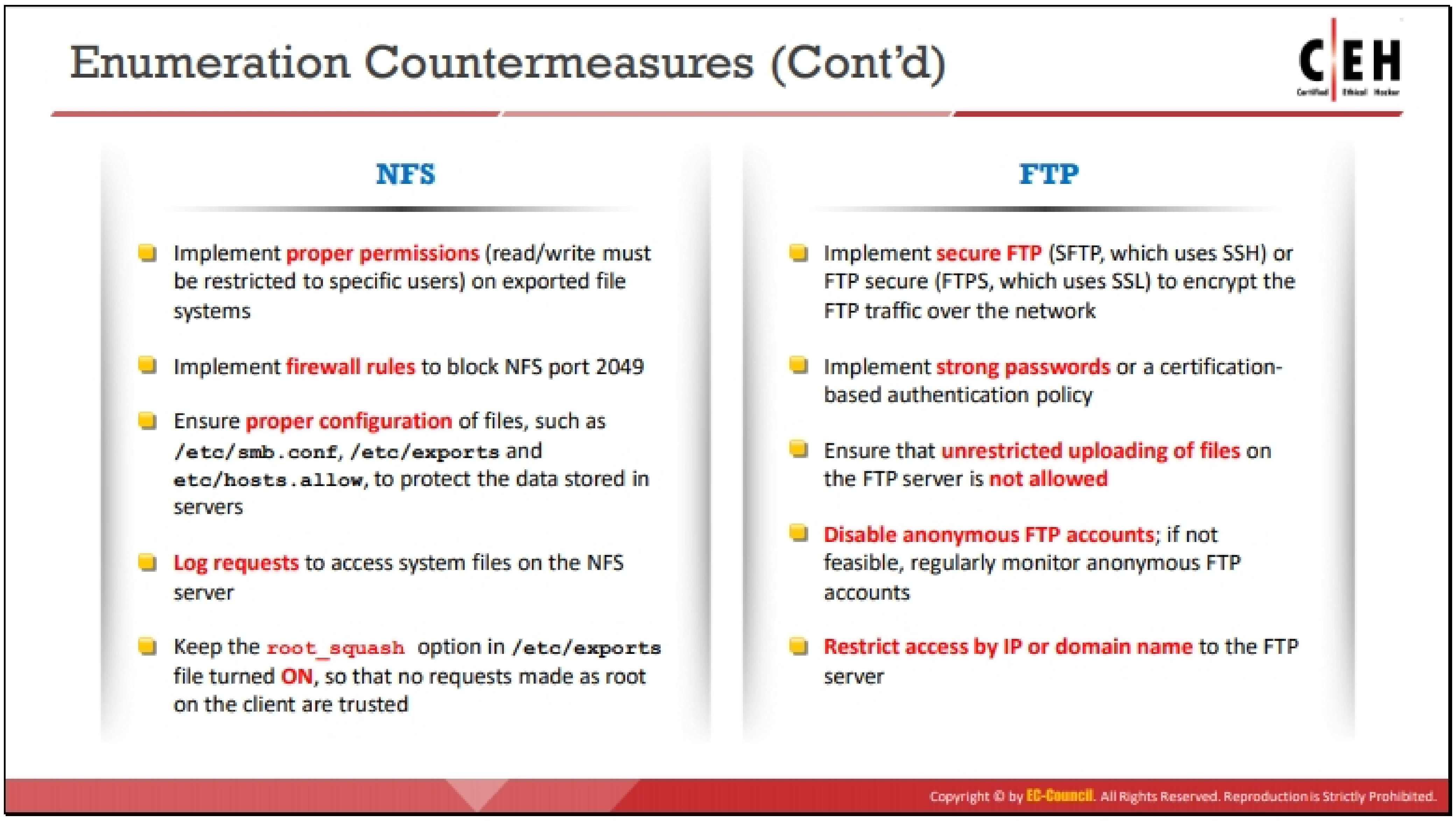
- Ignore **email messages** to unknown recipients
- Exclude sensitive **mail server** and **local host information** in mail responses
- Disable **open relay** feature
- **Limit the number of accepted connections** from a source to prevent brute-force attacks

LDAP

- By default, LDAP traffic is transmitted unsecured; **use SSL or STARTTLS technology** to encrypt the traffic
- Select a **username different** from your email address and enable **account lockout**
- Use **NTLM** or any basic authentication mechanism to limit access to legitimate users only

SMB

- Disable SMB protocol on **Web and DNS Servers**
- Disable SMB protocol on **Internet facing servers**
- Disable ports **TCP 139** and **TCP 445** used by the SMB protocol
- Restrict anonymous access through **RestrictNullSessAccess** parameter from the **Windows Registry**



Enumeration Countermeasures (Cont'd)

NFS

- Implement **proper permissions** (read/write must be restricted to specific users) on exported file systems
- Implement **firewall rules** to block NFS port 2049
- Ensure **proper configuration** of files, such as `/etc/smb.conf`, `/etc/exports` and `etc/hosts.allow`, to protect the data stored in servers
- **Log requests** to access system files on the NFS server
- Keep the `root_squash` option in `/etc/exports` file turned **ON**, so that no requests made as root on the client are trusted

FTP

- Implement **secure FTP** (SFTP, which uses SSH) or FTP secure (FTPS, which uses SSL) to encrypt the FTP traffic over the network
- Implement **strong passwords** or a certification-based authentication policy
- Ensure that **unrestricted uploading of files** on the FTP server is **not allowed**
- **Disable anonymous FTP accounts**; if not feasible, regularly monitor anonymous FTP accounts
- **Restrict access by IP or domain name** to the FTP server

Enumeration Countermeasures

Thus far, we have described enumeration techniques and tools used to extract valuable information from targets. Next, we discuss countermeasures that can prevent attackers from enumerating sensitive information from a network or host. This section focuses on methods to avoid information leakage through SNMP, DNS, SMTP, LDAP, SMB, NFS, and FTP enumeration.

SNMP Enumeration Countermeasures

- Remove the SNMP agent or turn off the SNMP service.
- If turning off SNMP is not an option, then change the default community string names.
- Upgrade to SNMP3, which encrypts passwords and messages.
- Implement the Group Policy security option called “Additional restrictions for anonymous connections.”
- Ensure that the access to null session pipes, null session shares, and IPsec filtering is restricted.
- Block access to TCP/UDP port 161.
- Do not install the management and monitoring Windows component unless required.
- Encrypt or authenticate using IPsec.
- Do not misconfigure the SNMP service with read-write authorization.

DNS Enumeration Countermeasures

- Disable DNS zone transfers to untrusted hosts.
- Ensure that the private hosts and their IP addresses are not published in the DNS zone files of the public DNS server.
- Use premium DNS registration services that hide sensitive information such as host information (HINFO) from the public.
- Use standard network admin contacts for DNS registrations to avoid social engineering attacks.
- Prune DNS zone files to prevent revealing unnecessary information.

SMTP Enumeration Countermeasures

SMTP servers should be configured in the following manner.

- Ignore email messages to unknown recipients.
- Exclude sensitive information on mail servers and local hosts in mail responses.
- Disable the open relay feature.
- Limit the number of accepted connections from a source to prevent brute-force attacks.
- Disable EXPN, VRFY, and RCPT TO commands or restrict them to authentic users.
- Ignore emails to unknown recipients by configuring SMTP servers.

LDAP Enumeration Countermeasures

- By default, LDAP traffic is transmitted unsecured; therefore, use Secure Sockets Layer (SSL) or STARTTLS technology to encrypt the traffic.
- Select a username different from the email address and enable account lockout.

- Restrict access to Active Directory by using software such as Citrix.
- Use NTLM or any basic authentication mechanism to limit access to legitimate users.

SMB Enumeration Countermeasures

Common sharing services or other unused services may provide doorways for attackers to break into a network's security. A network running SMB is at a high risk of enumeration. Since web and DNS servers do not require this protocol, it is advisable to disable it on them. The SMB protocol can be disabled by disabling the properties **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** in **Network and Dial-up Connections**. On servers that are accessible from the Internet, also known as bastion hosts, SMB can be disabled by disabling the same two properties of the **TCP/IP properties** dialog box. Another method of disabling the SMB protocol on bastion hosts, without explicitly disabling it, is by blocking the ports used by the SMB service. These are TCP ports 139 and 445.

Because disabling SMB services is not always a feasible option, other countermeasures against SMB enumeration may be required. Windows Registry can be configured to limit anonymous access from the Internet to a specified set of files. These files and folders are specified in the settings **Network access: Named pipes that can be accessed anonymously** and **Network access: Shares that can be accessed anonymously**. This configuration involves adding the RestrictNullSessAccess parameter to the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

The RestrictNullSessAccess parameter takes binary values, with 1 denoting enabled and 0 denoting disabled. Setting this parameter to 1 or enabled restricts the access of anonymous users to the files specified in the **Network access** settings.

The following are additional countermeasures for defending against SMB enumeration.

- Ensure that Windows Firewall or similar endpoint protection systems are enabled on the system.
- Install the latest security patches for Windows and third-party software.
- Implement a proper authentication mechanism with a strong password policy.
- Implement strong permissions to keep the stored information safe.
- Perform a regular audit of system logs.
- Perform active system monitoring to monitor the systems for any malicious incident.

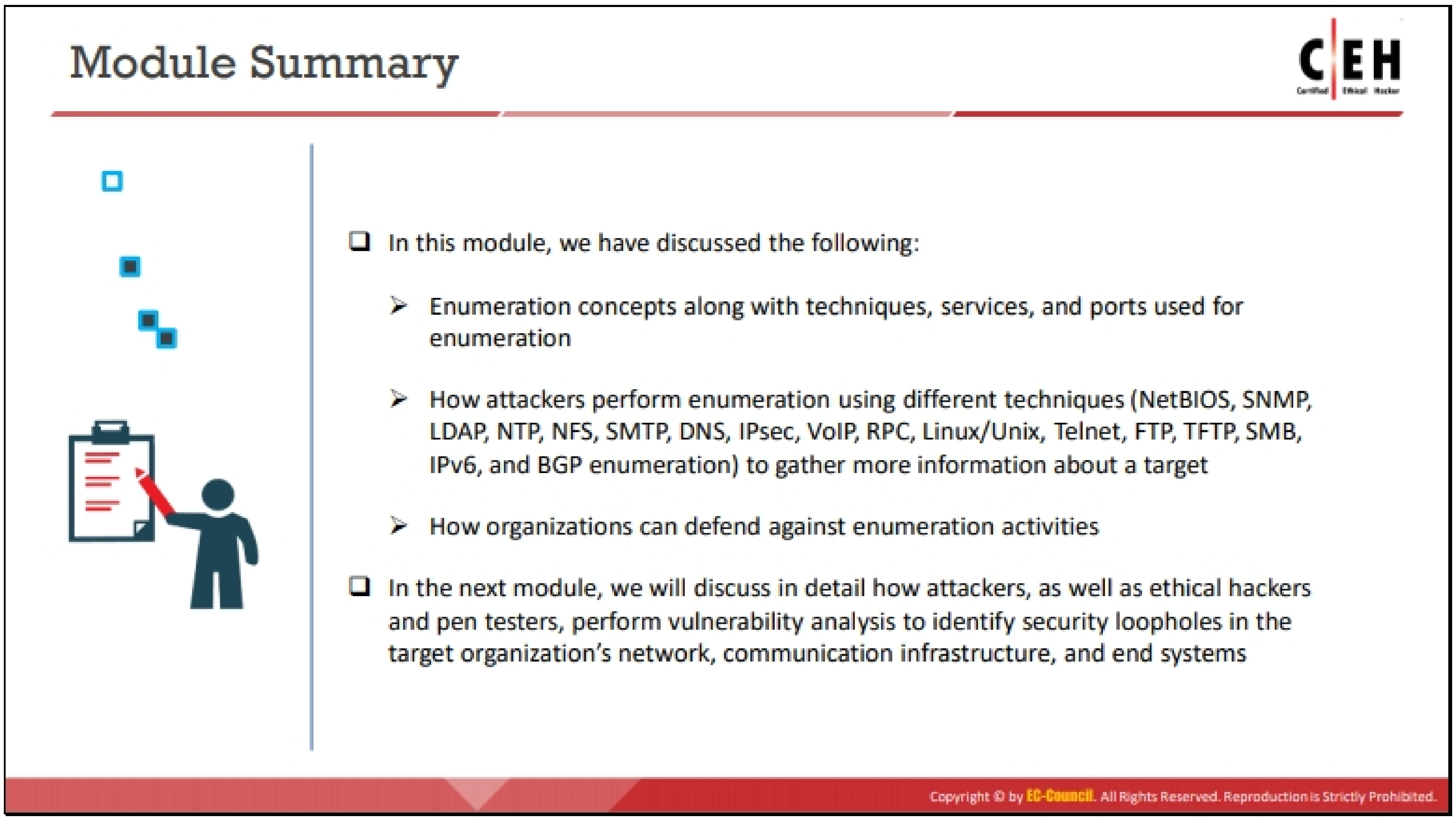
NFS Enumeration Countermeasures

- Implement proper permissions (read/write must be restricted to specific users) in exported file systems.
- Implement firewall rules to block NFS port 2049.
- Ensure the proper configuration of files such as `/etc/smb.conf`, `/etc/exports`, and `etc/hosts.allow` to protect the data stored in the server.

- Log the requests to access the system files on the NFS server.
- Keep the `root_squash` option in `/etc/exports` file turned **ON** so that no requests made as root on the client are trusted.
- Implement NFS tunneling through SSH to encrypt the NFS traffic over the network.

FTP Enumeration Countermeasures

- Implement secure FTP (SFTP, which uses SSH) or FTP secure (FTPS, which uses SSL) to encrypt the FTP traffic over the network.
- Implement strong passwords or a certification-based authentication policy.
- Ensure that the unrestricted uploading of files on the FTP server is not allowed.
- Disable anonymous FTP accounts. If this is not possible, monitor anonymous FTP accounts regularly.
- Restrict access by IP or domain name to the FTP server.
- Configure access controls on authenticated FTP accounts with the help of access control lists (ACLs).
- Restrict login attempts and time.
- Configure filtering rules for the FTP services.
- Use SSL/FTPS for authenticated FTP accounts.



Module Summary

- ❑ In this module, we have discussed the following:
  - ➢ Enumeration concepts along with techniques, services, and ports used for enumeration
  - ➢ How attackers perform enumeration using different techniques (NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration) to gather more information about a target
  - ➢ How organizations can defend against enumeration activities
- ❑ In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen testers, perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems

Module Summary

In this module, we discussed the enumeration concepts along with the techniques, services, and ports used for enumeration. We have also discussed how attackers perform different enumeration techniques (NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration) to gather information about the target. This module ended with a detailed discussion on the countermeasures that organizations can adopt to defend against enumeration activities.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen testers, perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.